



March 2017

IDENTITY THEFT SERVICES

Services Offer Some
Benefits but Are
Limited in Preventing
Fraud

Why GAO Did This Study

Private-sector and government entities that experience data breaches often provide affected consumers with identity theft services, which typically include credit monitoring, identity monitoring, identity restoration, and identity theft insurance. In response to data breaches in 2015, OPM awarded two contracts obligating about \$240 million for identity theft services.

GAO was asked to examine issues related to identity theft services and their usefulness. This report examines, among other objectives, (1) the potential benefits and limitations of identity theft services, and (2) factors that affect government and private-sector decision-making about them. GAO reviewed products, studies, laws, regulations, and federal guidance and contracts, and interviewed federal agencies, consumer groups, industry stakeholders, and eight providers selected because they were large market participants.

What GAO Recommends

Congress should consider permitting agencies to determine the appropriate coverage level for identity theft insurance they offer after data breaches. OMB should analyze the effectiveness of identity theft services relative to alternatives, and should explore options to address duplication in federal agencies' provision of these services. OPM should address in its breach-response policy when to offer these services and should document its decision-making process. OPM agreed with GAO's recommendations to the agency.

IDENTITY THEFT SERVICES

Services Offer Some Benefits but Are Limited in Preventing Fraud

What GAO Found

Identity theft services offer some benefits but have limitations.

- **Credit monitoring** helps detect new-account fraud (that is, the opening of new unauthorized accounts) by alerting users, but it does not prevent such fraud or address existing-account fraud, such as misuse of a stolen credit card number. Consumers have alternatives to credit monitoring, including requesting a low-cost credit freeze, which can prevent new-account fraud by restricting access to the consumers' credit report.
- **Identity monitoring** can alert consumers to misuse of certain personal information by monitoring sources such as public records or illicit websites, but its effectiveness in mitigating identity theft is unclear.
- **Identity restoration** seeks to remediate the effects of identity theft, but the level of service varies: some providers offer hands-on assistance, such as interacting with creditors on the consumer's behalf, while others largely provide self-help information, which is of more limited benefit.
- **Identity theft insurance** covers certain expenses related to the process of remediating identity theft but generally excludes direct financial losses, and the number and dollar amount of claims has been low.

These services also typically do not address some types of threats, such as medical identity or tax refund fraud.

Various factors affect government and private-sector decision making about offering identity theft services, and federal guidance related to these services could be improved. In the federal sector, legislation requires certain agencies to provide identity theft services. For example, legislation requires the Office of Personnel Management (OPM) to provide these services to individuals affected by its 2015 data breaches for 10 years, as well as provide \$5 million in identity theft insurance. However, this level of insurance coverage is likely unnecessary because claims paid rarely exceed a few thousand dollars. Requirements such as this could serve to increase federal costs unnecessarily, mislead consumers about the benefit of such insurance coverage, and create unwarranted escalation of coverage amounts in the marketplace. The Office of Management and Budget (OMB) has guidance on agencies' response to data breaches, but this guidance does not address the effectiveness of these services relative to lower-cost alternatives, in keeping with OMB's risk management and internal control guidance. Further, OPM provided duplicative identity theft services for about 3.6 million people affected by both of its 2015 breaches, and OMB has not explored options to help federal agencies avoid potentially wasteful duplication. In addition, contrary to key operational practices previously identified by GAO, OPM's data-breach-response policy does not include criteria or procedures for determining when to offer identity theft services, and OPM has not always documented how it chose to offer them in response to past breaches, which could hinder informed decision making in the future. In the private sector, companies often offer consumers affected by a data breach complimentary identity theft services for reasons other than mitigating the risk of identity theft, such as avoiding liability or complying with state law.

Contents

Letter		1
	Background	3
	A Number of Companies Provide Identity Theft Services to Millions of Consumers	5
	Services Offer Some Benefits but Do Not Prevent Identity Theft or Address Some of Its Variations	9
	Consumer Complaints and Enforcement Actions Have Focused on Billing and Marketing Issues among Some Providers	29
	Various Factors Affect Decision Making about Offering Identity Theft Services, and Federal Guidance Could Be Improved	35
	Conclusions	50
	Matter for Congressional Consideration	52
	Recommendations for Executive Action	52
	Agency Comments and Our Evaluation	52
Appendix I	Objectives, Scope, and Methodology	55
Appendix II	Selected Federal Laws Potentially Applicable to Identity Theft Services	60
Appendix III	Comments from the Office of Personnel Management	63
Appendix IV	GAO Contact and Staff Acknowledgments	65
Table		
	Table 1: Comparison of Paid and Free Credit Monitoring and Related Actions	14
Figure		
	Figure 1: Examples of How Personal Information Is Obtained and Used to Commit Identity Theft	5

Abbreviations

CFPB	Bureau of Consumer Financial Protection
DHS	Department of Homeland Security
FCRA	Fair Credit Reporting Act
FISMA	Federal Information Security Modernization Act of 2014
FTC Act	Federal Trade Commission Act
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
GSA	General Services Administration
IRS	Internal Revenue Service
OMB	Office of Management and Budget
OPM	Office of Personnel Management
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



March 30, 2017

Congressional Requesters

In recent years, many entities in the private and government sectors have experienced data breaches involving the loss or theft of sensitive personal information, such as Social Security and credit card numbers. Data breaches raise concern in part because they are one of the potential sources of information used for identity theft. In response to these breaches, many private-sector and government entities have provided affected consumers with identity theft services.¹ For example, a total of about \$240 million has been obligated as of January 2017 for identity theft services provided by the Office of Personnel Management (OPM) to approximately 22.1 million individuals affected by breaches of OPM databases containing background investigations and other personnel records. Recent legislation required OPM to provide these services for an increased length of time to individuals affected by certain data breaches.² Consumers can also purchase identity theft services directly from identity theft service providers.

You asked us to review issues related to identity theft services and their usefulness. This report examines (1) the marketplace for identity theft services; (2) the potential benefits and limitations of identity theft services available to consumers; (3) marketing, billing, and security issues associated with these services; and (4) factors that affect government and private-sector decision making about offering identity theft services.

To examine the identity theft services marketplace, we used Internet search techniques and keyword search terms to identify sources and types of available information about this market. We also reviewed

¹For the purposes of our review, we use the term "identity theft services" to refer to commercial products that generally provide tools intended to help consumers detect identity theft and restore their identity if it has been compromised. There is no standard term to describe these services, which sometimes are also referred to as "identity theft protection services," "identity protection services," "identity monitoring services," and "credit monitoring services," among other variations.

²Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, § 632, 129 Stat. 2242, 2470 (2015). The act required OPM to provide individuals affected by the two data breaches it announced in 2015 with complimentary identity protection coverage that is effective for a period of not less than 10 years. Prior to this legislation, the coverage provided by OPM for the two breaches was for 18 months and 3 years, respectively.

studies on identity theft services conducted by consumer advocacy groups, private research firms, and nonprofit organizations. In addition, we analyzed U.S. Census Bureau data on business classification codes related to identity theft services. On the basis of our analyses, we determined that the Census data do not provide a reliable count or other statistical information on the identity theft services industry, and limited public information exists about the industry as a whole. To examine the potential benefits and limitations of these services, we reviewed the websites of 26 identity theft service providers; the services' terms and conditions and insurance policies; and studies and reports that have highlighted their benefits and limitations. In addition, we reviewed reports that seek to rate and evaluate identity theft services that were issued by consumer groups, private research firms, and industry analysts. To examine marketing, billing, and security issues associated with identity theft services, we reviewed federal enforcement actions and collected and analyzed consumer complaints received by the Federal Trade Commission (FTC), the Bureau of Consumer Financial Protection (CFPB), and the Better Business Bureaus. We assessed the reliability of the complaint data by interviewing agency officials, analyzing complaint narratives, and comparing data from the three different sources. We found the data to be reliable for purposes of this reporting objective.

To assess government and private-sector decision making about offering identity theft services, we reviewed documentation from, and interviewed representatives of, OPM and other selected federal and private entities that have purchased these services for affected consumers in response to data breaches. The factors considered in selecting these entities included the number of records breached, sensitivity of the data breached, when the breach took place, and whether identity theft services were procured as a result. We also reviewed relevant laws and regulations, federal guidance, federal data breach policies, and contract documentation. For all objectives, we interviewed officials from federal agencies, consumer advocacy groups, trade associations, and experts in security or identity theft services. These entities and individuals were selected because of their involvement and expertise in the area of identity theft services. We also interviewed representatives from a nongeneralizable sample of eight companies that provide identity theft services, which were selected to include large market participants and a mix of product offerings. Appendix I describes our objectives, scope, and methodology in greater detail.

We conducted this performance audit from September 2015 to March 2017, in accordance with generally accepted government auditing

standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Identity theft occurs when individuals' identifying information is used without authorization in an attempt to commit fraud or other crimes. Identity thieves obtain sensitive personal information—which can include personally identifiable information such as Social Security numbers or financial information such as credit card numbers—using a variety of methods.³ One potential source of identity theft is a data breach at an organization that maintains large amounts of sensitive personal information, although data breaches do not necessarily result in identity theft. Another method of identity theft involves tricking individuals or employees of an organization to share their own or others' sensitive personal information. Identity theft can also occur as a result of the loss or theft of data maintained by an individual, such as a lost or stolen wallet or a thief digging through household trash. While these stolen data are commonly used to commit financial crimes, they can also be used for other purposes, such as espionage, information warfare, or terrorism.

As seen in figure 1, identity theft can include existing-account fraud and new-account fraud.

- **Existing-account fraud** occurs when identity thieves use financial account identifiers, such as credit card or debit card numbers, to take over an individual's existing accounts to make unauthorized charges or withdraw money. While this form of identity theft is a significant problem, existing laws limit consumer liability for such fraud and, as a

³For the purposes of this report, unless otherwise noted, we use "personally identifiable information" to refer to any information that can be used to distinguish or trace an individual's identity—such as name, Social Security number, driver's license number, and mother's maiden name—but not to refer to account-specific information, such as credit or debit card numbers.

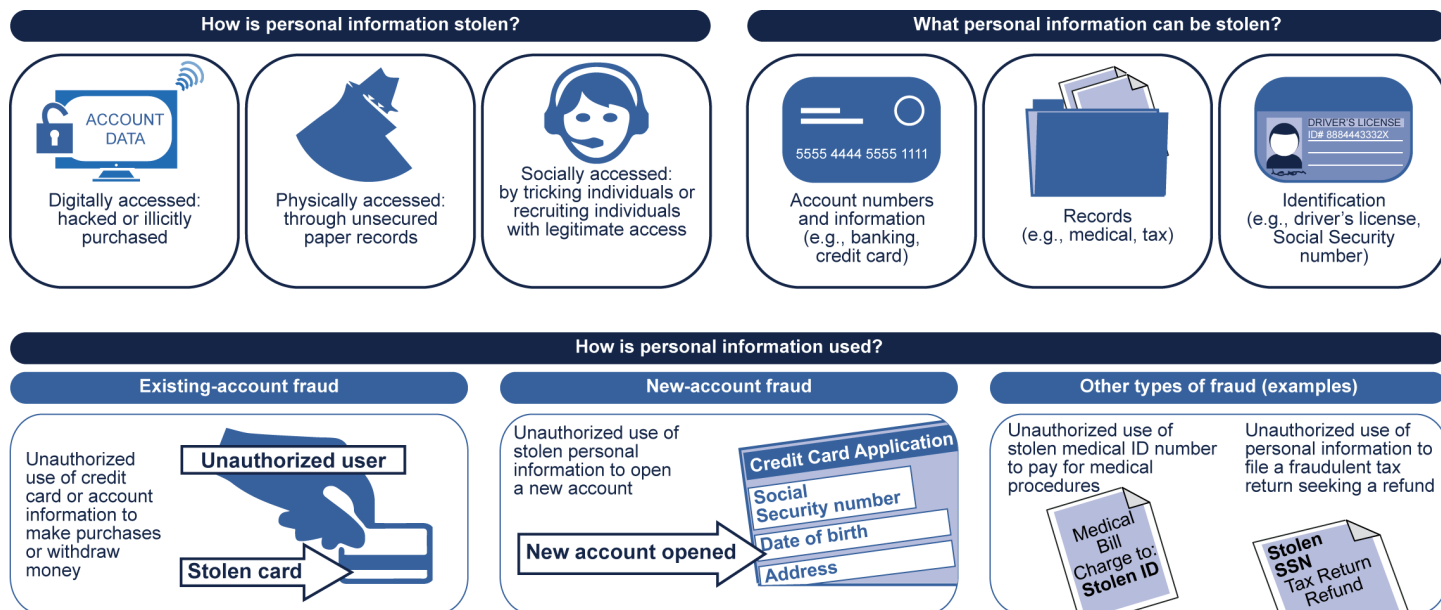
matter of policy, some credit and debit card issuers may voluntarily cover all fraudulent charges.⁴

- **New-account fraud** occurs when thieves use identifying data, which can include such information as Social Security and driver's license numbers, to open new financial accounts and incur charges and credit in an individual's name without that person's knowledge. New-account fraud is potentially the most damaging form of identity theft because, among other things, a credit card or bank account number can be changed, but it is difficult or impossible to replace information such as Social Security numbers and date of birth. In addition, some time may pass before a victim becomes aware of the problem, and fraudulent accounts can cause substantial harm to the victim's credit rating.

More recent and growing forms of identity theft include, among others, medical identity theft (using someone else's identity to obtain medical services or submit fraudulent insurance claims); identity theft return fraud (filing tax returns under a false identity to fraudulently obtain a refund); and synthetic identity theft (creating a fictitious identity, typically by combining real data from multiple individuals and fabricated information).

⁴For unauthorized credit card charges, cardholder liability is limited to a maximum of \$50 per account. 15 U.S.C. § 1643. For unauthorized automated teller machine or debit card transactions, the Electronic Fund Transfer Act limits consumer liability, depending on how quickly the consumer reports the loss or theft of the card. 15 U.S.C. § 1693g. Consumers also may incur additional costs if they fail to notice and report fraudulent charges and inadvertently pay them. In addition, account fraud can cause inconvenience or temporary hardship, such as losing temporary access to account funds or requiring the cancellation and reactivation of cards and the redirecting of automatic payments and deposits.

Figure 1: Examples of How Personal Information Is Obtained and Used to Commit Identity Theft



Source: GAO. | GAO-17-254

A Number of Companies Provide Identity Theft Services to Millions of Consumers

Although available data about the identity theft services industry are limited, a number of companies provide these services to millions of consumers. The private research firm IBISWorld estimated that the U.S. market for identity theft services was about \$3 billion in 2015 and 2016.⁵ Our review indicated there were about 50 to 60 companies providing these services as of 2015, according to private research firms, industry stakeholders, and our own analysis. Characterizing the precise size of the market, the number of subscribers, and other factors can be difficult, and no agency or trade association that we identified collects comprehensive data on the industry. For example, the U.S. Census Bureau does not assign a business classification code specific to identity theft services.⁶ Instead, the Census Bureau has assigned identity theft services as part of

⁵IBISWorld, *Identity Theft Protection Services in the US: Market Research* (April 2015), accessed December 10, 2015, <http://www.ibisworld.com/industry/identity-theft-protection-services.html>; and *Identity Theft Protection Services in the US: Market Research* (April 2016), accessed August 16, 2016, <http://www.ibisworld.com/industry/identity-theft-protection-services.html>.

⁶The Census Bureau assigns business classification codes, including Standard Industrial Classification and North American Industry Classification System codes, to each company to classify its main industry and line of business.

a broader code—"all other personal services"—that contains about 50 different personal services from astrology services to wedding planning. Thus, Census data cannot be used to provide a reliable count or other statistical information on the identity theft services industry as a whole. Furthermore, representatives of CFPB, FTC, and the identity theft services industry told us they had not collected and were not aware of comprehensive data on the number of subscribers or overall market landscape of the industry. One of the largest providers reported in its public filings that it had 4.2 million subscribers in 2015, and another large provider reported it had nearly 1.2 million subscribers in 2015. Large market participants include companies whose primary line of business is identity theft services and other companies that include consumer reporting agencies (also known as credit bureaus) and cybersecurity companies.⁷

While identity theft services vary, most often they include four types: (1) credit monitoring (which monitors the user's credit report); (2) identity monitoring (which tracks personal data in sources such as public records or illicit websites); (3) identity restoration (which assists in recovering from identity theft); and (4) identity theft insurance (which reimburses certain costs related to the process of restoring one's identity). Providers of identity theft services sell products through various channels, including directly to consumers, in partnership with financial service or other companies as an added service, as a service to victims of a data breach, or as an employee benefit. Some providers focus on selling directly to consumers, while some specialize in selling post-data-breach services to breached entities, and some providers market their services to both categories. It is common for providers to sell identity theft services as part of a package of post-data-breach services that can also include breach notification and call-center support. Providers also partner with other companies that have expertise in cybersecurity or restoration services so that one company markets the services to consumers or secures contracts, and the other company provides the services.

Nearly all of the 26 identity theft service providers whose websites we reviewed sold directly to consumers, although there are limited data on the overall size of the direct-to-consumer market. Javelin Strategy & Research found that consumers spent over \$1.4 billion on identity theft

⁷Consumer reporting agencies—including the three largest nationwide credit bureaus, Equifax, Experian, and TransUnion—provide consumers with reports that commonly are used to determine eligibility for credit, employment, and insurance.

subscriptions between late 2013 and 2014—although it reported that nearly a third of all subscribers withdrew from the direct-to-consumer market in 2014.⁸ According to the Department of Justice’s Bureau of Justice Statistics, in 2014 about 5 percent of adults (aged 16 or older) purchased credit monitoring services or identity theft insurance, and 3.5 percent purchased identity theft protection—nearly the same percentages reported for 2012.⁹

Among the 26 providers we reviewed, some offered one standard product package, while others offered consumers a choice of 2 or more packages that had different prices and slightly different features, although one provider told us it offered more than 40 different packages. Packages ranged from about \$5–\$30 a month. Among five large providers from that group whose price structure we reviewed in greater detail, prices varied, but all had at least one package priced at about \$16–\$20 a month. One of the largest providers reported in its public filings that its monthly average revenue per member was about \$12 per person per month. The differences between a provider’s various packages can include whether credit reports are monitored at one, two, or all three of the nationwide credit bureaus; whether identity monitoring is included; whether the package is for an individual or family; and whether additional features are included, such as credit scores or tools to protect personal computers. As with many types of commercial products, we found that prices sometimes differed for the same product based on where it was marketed—for example, whether the consumer enrolls on the provider’s main webpage versus a different webpage where the provider offers promotional prices.

⁸Javelin Strategy & Research, *Identity Protection Direct-to-Consumer Services Reach \$1.4B in a Year Ridden with Data Breaches* (April 2015), accessed September 21, 2016, <https://www.javelinstrategy.com/press-release/identity-protection-direct-consumer-services-reach-14b-year-ridden-data-breaches>. Javelin Strategy & Research is a research-based consulting firm that focuses on retail and small-business banking. This study surveyed a random-sample online panel of 3,100 respondents in August and September 2014 and a random-sample panel of 5,000 respondents in November and December 2014.

⁹Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* (September 2015). Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (December 2013). Adults were defined as age 16 or older. The survey associated with the studies asked two separate questions related to individuals’ purchase of identity theft services. The first question asked about the purchase of credit monitoring or identity theft insurance, and the second question asked about the purchase of identity theft protection services. The results of these questions are reported separately, but there may be some overlap in the answers due to the similarity of the services. Therefore, the reported results cannot be combined.

In addition, it has become common practice for entities experiencing a data breach to provide complimentary identity theft services to individuals whose personal information was compromised. A study by the RAND Corporation found that individuals who had received a breach notification were offered free identity theft services after a data breach about 60 percent of the time, and Javelin Strategy & Research estimated that data breaches accounted for one out of every five identity theft service subscriptions in 2015.¹⁰ In recent years, several federal agencies and some of the nation's largest retailers, health insurers, and other companies have provided consumers with identity theft services after experiencing data breaches. In just five large breaches reported between 2013 and 2015, free identity theft services were offered to affected individuals a total of about 340 million times.¹¹

Providers generally told us that the pricing structure for services offered to entities post data breach varies based on the size of the affected population and the services selected. Due to these variations, and the proprietary nature of the information, providers generally did not provide us with the exact prices they charge companies for post-data-breach services. In general, they indicated that wholesale prices for breached entities were lower than those sold directly to consumers. A representative of one identity theft service told us that a company might pay between \$4 and \$15 per year for each consumer affected by the breach, independent of how many of those consumers choose to enroll in the service. One study by an insurance company estimated that identity theft services can cost companies between \$10 and \$30 per year per affected individual.¹²

¹⁰Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information* (Santa Monica, Calif.: RAND Corporation, 2016), 22. The RAND Corporation is a nonprofit, public interest research organization. The study surveyed about 2,600 adults (over the age of 18) in May and June of 2015. Javelin Strategy & Research, *IDPS: Changing Suit of Armor to Match ID Victims' Needs* (June 2016), accessed June 24, 2016, <https://www.javelinstrategy.com/blog/idps-changing-suit-armor-match-id-victims'-needs>.

¹¹This figure does not represent individual persons because the same person may have been offered services by more than one entity. In addition, only a portion of those offered complimentary identity theft services actually enroll.

¹²Zurich Insurance Company, *The Good, the Bad and the Careless: An Overview of Corporate Cyber Risk* (Zurich, Switzerland: Zurich Insurance Company Ltd, 2014), 7.

Prices for post-data-breach identity theft services marketed to the federal government can be found in the General Services Administration's (GSA) Identity Protection Services Multiple Award Blanket Purchase Agreement.¹³ Agreements we reviewed provided several pricing options to agencies, including the option of paying either a fixed overall fee or paying a fee based on the number of consumers who enroll in the service. For example, one contractor charges either about \$10 per person annually to cover all affected individuals with a full scope of services, or \$38 to \$52 annually (range based on volume) for each person who actually enrolls. Another contractor charges federal agencies \$10 to \$49 per person annually for services, with the price varying based on the specific services offered.

Services Offer Some Benefits but Do Not Prevent Identity Theft or Address Some of Its Variations

Identity theft services offer some benefits but generally do not prevent identity theft or address all of its variations. The services typically include one or more of the following: credit monitoring, identity monitoring, identity restoration, and identity theft insurance. However, these services typically do not address medical identity theft, identity theft refund fraud, and certain other threats involving stolen personal information. Evaluation and analysis of these services by both federal and private-sector entities is limited and tends to focus on outputs (such as contractor performance) rather than outcomes (such as reduction of harm from identity theft).

Credit Monitoring Can Detect New-Account Fraud, but Free and Low-Cost Alternatives Exist That Can Prevent It

All but 3 of the 26 identity theft service providers whose websites we reviewed provided some level of credit monitoring. Credit monitoring tracks consumers' credit reports to help identify suspicious activity that could be a result of identity theft.¹⁴ A credit monitoring service typically alerts consumers—by telephone, mail, text, e-mail, or other messaging technologies—to changes in their credit report, such as when a new loan

¹³A blanket purchase agreement is a contracting vehicle that agencies are encouraged to use in order to easily access and acquire qualified providers on prenegotiated prices for these services. It is a simplified method of filling anticipated repetitive needs for supplies or services by establishing "charge accounts" with qualified sources of supply. 48 C.F.R. § 13.303-1(a).

¹⁴Credit reports are compiled from businesses that offer credit and from other sources and are provided, generally for a fee, to consumers and other businesses. Lenders rely on credit reports when deciding whether to offer credit to an individual, at what rate, and on what terms. In addition, potential employers, insurance underwriters, and landlords sometimes use credit reports to assess applicants' creditworthiness or other characteristics.

or credit card account is opened in the consumer's name or a creditor reports a late payment. These alerts allow consumers to determine whether a change is legitimate or whether it indicates possible fraudulent use of their personal information. Most identity theft services monitor activity on a consumer's credit report at one or at all three of the nationwide credit bureaus—Equifax, Experian, and TransUnion.¹⁵

Credit Monitoring Can Detect New-Account Fraud

The primary benefit of credit monitoring is to alert the consumers of new-account fraud—that is, fraud involving new accounts that are opened using their personal information. Consumers alerted to a change in their credit report that they do not recognize can investigate whether someone used their personal information to open a new credit account or commit other acts of fraud. Early detection of new-account fraud allows for more effective mitigation, such as closing the fraudulent account, requesting a fraud alert or credit freeze, and beginning the process of correcting and restoring the victim's credit record. The service can offer convenience by facilitating credit report monitoring without the need for a consumer to be proactive and check their credit reports for changes. In addition, credit monitoring typically monitors credit reports on an ongoing basis, sometimes notifying the customer of changes within a day or less. By contrast, several months may pass before consumers detect fraud by reviewing their credit reports on their own. In addition, because credit monitoring often covers all nationwide credit bureaus, it may alert consumers to changes or inquiries that they would not catch if they were reviewing their report from just one of the bureaus.

Credit Monitoring Does Not Prevent Fraud, but Free and Low-Cost Alternative Tools Do

While credit monitoring can *detect* new-account fraud, its scope is limited because it does not *prevent* such fraud. Credit monitoring alerts consumers only after-the-fact to potential fraudulent use of personal information to open a new credit account. One consumer group has expressed concern that consumers may not understand this limitation, particularly because product marketing sometimes states that the services “protect” one's identity and the products themselves are commonly referred to as identity protection services. FTC warns

¹⁵We use “nationwide credit bureau” to refer to what the Fair Credit Reporting Act (FCRA) defines as a “consumer reporting agency that compiles and maintains files on consumers on a nationwide basis.” FCRA defines this phrase as a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining public record information and credit account information regarding consumers residing nationwide for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity. 15 U.S.C. § 1681a(p).

consumers that no service can protect you from having your personal information stolen.¹⁶

However, as an alternative to credit monitoring, there are two free or low-cost tools—fraud alerts and credit freezes—that can prevent new-account fraud, according to federal agencies, consumer groups, and others. When a fraud alert is in place at a credit bureau, a business must verify a consumer's identity before it issues credit, which can make it harder for an identity thief to open accounts in the consumer's name.¹⁷ Some identity theft services assist consumers with fraud alerts, but may face limitations in their ability to request or extend fraud alerts on behalf of a consumer.¹⁸ A credit freeze, sometimes referred to as a security freeze, restricts potential creditors from accessing a consumer's credit report until the consumer asks the credit reporting company to remove or temporarily lift the credit freeze.¹⁹ These tools can prevent new-account fraud because creditors generally will not extend credit without first checking a consumer's credit report. Some consumer groups have advocated that consumers paying for credit monitoring consider requesting a credit freeze instead. While a credit freeze is an effective tool to mitigate identity theft risk, CFPB, FTC, and others have noted that a credit freeze may not be the right choice for all consumers because it can slow the process of

¹⁶Federal Trade Commission, *Consumer Information: Identity Theft Protection Services*, accessed December 5, 2016, <https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services>.

¹⁷Consumers can request an initial fraud alert, extended fraud alert, or active duty alert at no cost with any one of the three nationwide consumer reporting agencies, which automatically must notify the other two. An initial fraud alert stays on the victim's credit file for 90 days and can be renewed every 90 days. An extended fraud alert, which lasts for 7 years, is available to victims of identity theft who have filed a formal identity theft report with one of the nationwide credit bureaus. Active duty alerts, which last for 1 year, are available to deployed service members. 15 U.S.C. § 1681c-1.

¹⁸For example, in 2009, a federal district court granted a credit reporting organization partial summary judgment, finding that a corporation's business practice of requesting national consumer reporting agencies to place fraud alerts on consumer files violated California law because it was against public policy established by the Fair Credit Reporting Act. *Experian Info. Solutions, Inc. v. Lifelock, Inc.*, 633 F. Supp. 2d 1104, 1008 (C.D. Cal. 2009).

¹⁹State law generally allows for and governs credit freezes. While state laws vary, a credit freeze generally allows consumers to request a freeze on their credit reports by contacting each of the nationwide consumer reporting agencies and paying a fee, typically \$5–\$10 to each agency. Consumers are given a unique personal identification number or password that they use to temporarily lift or remove the freeze (for example, when they are applying for credit or employment). A consumer reporting agency generally must lift a freeze no later than 3 business days after getting the consumer's request.

Credit Monitoring Does Not Address Existing Account Fraud

obtaining credit while potential creditors wait for the consumer to affirmatively lift the freeze. FTC and CFPB have cited evidence that many consumers are unaware of the option provided under state law to freeze their credit, and that some consumers who are aware of the option are confused by the process.²⁰

The scope of credit monitoring is further limited in that it does not alert consumers to existing-account fraud—that is, fraud associated with credit card, bank, or other accounts that already exist. According to the Bureau of Justice Statistics, the vast majority of identity theft victims are victims of existing-account fraud.²¹ Consumers typically learn of existing-account fraud when they review their bank or credit card statements, or when their financial institution alerts them of a suspicious charge or activity. Credit monitoring does not alert consumers to unauthorized charges or withdrawals because such charges are not reflected as a change or inquiry to one's credit report. In a notice to consumers, FTC notes the limitations of credit monitoring, reminding consumers that credit monitoring only warns about activity appearing on a credit report and does not, for example, notify consumers of an unauthorized bank account withdrawal or misuse of a Social Security number to file a tax return. Other examples of identity theft that credit monitoring may not detect include use of personal information to fraudulently obtain electricity or cable services, fraudulent wire transfers, or fraudulent withdrawal from a retirement or brokerage account. A representative from an industry association representing consumer reporting agencies and an identity theft service provider noted that, in some instances, credit monitoring may

²⁰For example, FTC has noted that a 2012 survey it commissioned suggested that a relatively small percentage of identity theft victims were aware of their rights under the Fair Credit Reporting Act, which include the right to a fraud alert. Additionally, CFPB has said that feedback it has received from federal and state officials and consumer groups suggested that many consumers were unaware of the option to freeze their credit, which as noted previously, is generally governed by state law. FTC and CFPB both discussed potential ways to streamline the credit freeze process, such as allowing consumers to request a freeze at all three credit bureaus by contacting only one. Letter from Edith Ramirez, Chairwoman of FTC, to Fred Upton, Chairman, House Committee on Energy and Commerce (Aug. 14, 2015). Letter from Richard Cordray, Director of CFPB, to Fred Upton, Chairman, House Committee on Energy and Commerce (Dec. 3, 2015).

²¹Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* (September 2015). In 2014, 90.8 percent of identity theft victims reported one or more of the following: unauthorized use of a credit card, bank account, or other form of existing-account fraud. About 3.9 percent reported only new-account fraud, and an additional 2.1 percent reported multiple types of identity theft that may have included existing-account fraud or new-account fraud. The data were based on 64,287 respondents to the Identity Theft Supplement of the National Crime Victimization Survey.

Consumers Have No-Cost Alternatives to Monitor Their Credit Reports

help consumers detect credit card account fraud if fraudulent charges result in a significant increase in a credit card's balance that is reflected in a credit report. However, the added value of this benefit is unclear given that individuals can already check their account directly, and credit card companies' fraud prevention departments already alert consumers of unusual activity that may indicate fraud.²²

FTC, CFPB, consumer groups, and others have noted alternative ways that consumers can monitor their credit report in lieu of a paid credit monitoring service. As discussed earlier, credit monitoring is typically provided as part of a package of services that usually range in cost from \$10–\$30 per month (\$120–\$360 annually). However, consumers can monitor their credit themselves at no cost by periodically reviewing their credit reports. Federal law requires each of the three nationwide consumer reporting agencies (often known as credit bureaus) to provide one free credit report to consumers, upon request, each year.²³ By spreading out these requests, consumers can review one free report every 4 months. Consumers also can receive a free annual credit report from the nationwide specialty consumer reporting agencies that sell information about, for example, check writing histories and rental history records.²⁴ However, it is unclear to what extent consumers fully understand that they are entitled to free credit reports. In a December 2012 study, CFPB estimated that 15.9 million consumers had obtained free annual credit reports through the authorized website, AnnualCreditReport.com, compared to 26 million consumers who had obtained their credit reports through a credit monitoring service. FTC and others have suggested that consumers take advantage of the free credit monitoring that is sometimes offered after a data breach or in conjunction with credit cards or other services. FTC, the Consumer Federation of America, and others also recommend that consumers regularly review account statements to alert them to fraudulent charges. Table 1 shows

²²In addition, some credit card companies offer customers the option of being alerted when an individual charge, or the overall balance, exceeds a certain amount. At least one identity theft service provider offers a similar service, via a mobile application that alerts consumers to suspicious transactions posted to their credit cards, debit cards, or bank accounts, as well as if the consumer had used a card at a retailer during a period of heightened risk due to a known data breach.

²³15 U.S.C. § 1681j(a); 12 C.F.R. § 1022.136. The authorized website for ordering free credit reports from the nationwide credit bureaus is AnnualCreditReport.com.

²⁴15 U.S.C. § 1681j(a); 12 C.F.R. § 1022.137.

some of the key differences between credit monitoring and other related alternatives.

Table 1: Comparison of Paid and Free Credit Monitoring and Related Actions

Tool or Service	Description	Prevents new-account fraud	Detects new-account fraud	Detects existing-account fraud	Monitoring convenient and frequent	Free or low-cost
Paid credit monitoring service	Fee-based service that tracks credit report to alert consumer of suspicious activity		✓		✓	
Free credit monitoring service	Credit monitoring offered to consumers at no charge, either by a breached entity or by a company marketing other services ^a		✓		✓	✓
Self-review of free annual credit reports	Consumer reviews credit reports provided free annually by each of the three nationwide credit bureaus and the nationwide specialty consumer reporting agencies		✓			✓
Self-review of credit card and bank statements	Consumer reviews statements for suspicious activity			✓		✓
Credit freeze	Restricts potential creditors from accessing credit report until the consumer temporarily lifts or removes the credit freeze	✓				✓
Fraud alert	Requires potential creditors to verify applicant's identity	✓				✓

Source: GAO. | GAO-17-254

^aAlthough services offered by a breached entity are free to the consumer, the entity itself incurs costs in contracting for these services.

We did not identify data on the effectiveness of paid credit monitoring services in alerting consumers to identity theft. According to the Department of Justice's Bureau of Justice Statistics, about 1.4 percent of victims in 2014 discovered identity theft through a credit report or credit

monitoring service.²⁵ One consumer group has expressed concern that credit monitoring services create “false alarms” for consumers because most alerts reflect routine and legitimate changes in consumers’ credit files. Additionally, 10 of the 26 providers we reviewed monitor all three credit bureaus as part of their standard service, with 9 others providing the option to monitor three bureaus as an enhanced service. FTC and some consumer groups have noted that services that monitor only one credit bureau may miss some potential fraud because not all credit transactions are reported to all three bureaus.

Identity Monitoring Can Alert Consumers to Some Misuse of Personal Information, but Its Effectiveness Is Unclear

Most identity theft services whose websites we reviewed indicated that they provided identity monitoring, although specific features varied. Identity monitoring services monitor sources other than credit reports, including public records, proprietary databases, and black-market websites used to buy and sell information illegally. The services scan these sources for a consumer’s personal information, such as names, addresses, and e-mail addresses, as well as credit card, Social Security, driver’s license, passport, and medical insurance numbers. The services typically alert consumers when they detect new or inaccurate information about them or detect their personal information in an inappropriate place, such as a black-market website.

Given the limited scope of credit monitoring, many providers with whom we spoke believed that identity monitoring was an important element of an identity theft service, and these providers, FTC, one consumer group, and a trade association identified the following benefits:

- **Addresses risks not detected in a credit report.** Identity monitoring can address forms of fraud that would not be revealed through credit monitoring.²⁶ For example, monitoring criminal and arrest record databases and sex offender lists can detect when a consumer’s

²⁵Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* (September 2015). The survey found that the most common way victims discovered identity theft was by being contacted by a financial institution (about 45 percent). For identity theft other than existing account fraud (including new account fraud), about 5.9 percent of victims said they discovered the theft through a credit report or credit monitoring service.

²⁶Most consumer identity theft complaints overall in 2015 did not involve new-account fraud, which credit monitoring is designed to detect, according to our review of FTC’s summary of consumer complaints. Federal Trade Commission, *Consumer Sentinel Network Data Book for January-December 2015* (Washington, D.C.: February 2016).

identity was falsely provided to police. Further, monitoring illicit websites can reveal misuse of e-mail addresses, user names, and passwords.

- **Can provide early detection and mitigation.** Identity monitoring does not typically prevent the theft of personal information, but it can serve as an early warning mechanism for consumers to take action before the information is misused for fraudulent purposes. For example, some services monitor the U.S. Postal Service's change-of-address database so that consumers can correct changes made by someone trying to improperly redirect their mail.²⁷ Similarly, consumers can change passwords that are discovered for sale on black-market websites.
- **Provides a service consumers cannot readily perform themselves.** Identity monitoring services scan sources that a consumer may have difficulty scanning themselves (such as public records) or may not have access to (such as black-market websites).

However, we did not identify any studies or data assessing the effectiveness of identity monitoring. One provider said that monitoring could be evaluated using information on the number of "hits" their service detects on sources such as black-market websites, but noted that this information could be difficult to interpret because many of the hits are not the results of fraud.²⁸ In addition, it is not clear how much risk individual consumers face when their personal information has been found on a black-market website. FTC has advised consumers that the effectiveness of identity monitoring depends on factors such as the kinds of databases the service provider monitors, how good the databases are at collecting information, and how often the service provider checks each database.²⁹

Furthermore, some consumer groups have expressed skepticism about the usefulness of identity monitoring, and these consumer groups and FTC noted the following limitations:

²⁷Identity thieves can use change-of-address cards to reroute mail to themselves, thereby capturing personal information.

²⁸For example, this provider said that their services detected that about 18 percent of its customers under one contract had e-mail addresses, passwords, or other credentials discovered on black-market websites.

²⁹Federal Trade Commission, *Consumer Information: Identity Theft Protection Services*, accessed September 23, 2016, <https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services>.

-
- **Some types of fraud are not monitored.** Some types of fraud are unlikely to be detected by identity monitoring—including debit or check card fraud, tax refund fraud, and medical identity theft. Some consumer groups say that identity monitoring can provide a false sense of security to consumers who do not understand its limitations.
 - **Mitigation is sometimes unclear.** While passwords or account numbers discovered for sale on black-market websites can be changed or cancelled, it is not always clear what actions, if any, consumers should take when more permanent information, such as a Social Security number, is discovered.

Identity Restoration Providers Vary in Their Level of Service

All 26 of the providers whose websites we reviewed stated that they provided some level of identity theft restoration—sometimes referred to as identity recovery or resolution—which is designed to help consumers regain control of their identity and finances after identity theft occurs. Some providers we spoke with characterized identity restoration as restoring a victim's identity to pre-event status or correcting an individual's records to reverse the effects of the fraud. Identity restoration services, when comprehensive, can help victims of identity theft by offering expert assistance and guidance in the steps needed to resolve problems and restore one's identity, according to stakeholders with whom we spoke.

Resolving identity theft can involve a number of steps that some consumers may have difficulty taking without assistance, such as contacting financial institutions to dispute fraudulent accounts or contacting credit bureaus to report errors or place a fraud alert. The services can save consumers the time it would take for them to take these steps themselves. They can also help consumers who may find it difficult to take the needed steps, such as some individuals who have cognitive or physical limitations or limited English proficiency. Some stakeholders we spoke with said that given the difficulty of preventing identity theft, and the benefit of having a service available in the event that an individual's identity is stolen—restoration services may be identity theft services' most important benefit.

However, identity restoration service providers vary substantially in the level of service provided. A review of 16 identity theft service providers' websites by the Consumer Federation of America found that some companies took an active role in providing fraud assistance to their customers, while most companies directed customers to a kit of materials and provided them with advice to resolve problems on their own. Similarly, our review of the websites of 26 providers—as well as

interviews with staff at 8 of these providers—found variations in the level of assistance provided to customers who had experienced identity theft. Sixteen of the 26 providers we reviewed noted they offered hands-on assistance, taking on tasks that consumers would otherwise need to do themselves. All 8 of the providers we spoke with told us they provided clients with an agent or specialist who conducts many of the steps to restore the victim’s identity. For example, these providers may use limited power of attorney to notify relevant federal agencies, such as the Internal Revenue Service (IRS) regarding identity theft refund fraud; work as needed with affected banks, credit card companies, collection agencies, check clearinghouse companies, landlords and property managers; and review criminal and other public records to determine the extent of the fraud. In addition, nearly all of these providers stated that their restoration agents or specialists received some specialized training, and one said it used only licensed investigators.

In contrast, other restoration services appeared to consist largely of a call center that provided consumers information to help them take action on their own. For example, one provider offered telephone support but focused on providing a “customized information kit so you can rectify the situation expediently.” Another advertised that it provided guidance to “advise you on any next steps you should take” with lenders or law enforcement authorities. However, similar guidance is available for free through FTC’s website IdentityTheft.gov. The website provides identity theft victims with free personal recovery plans that walk them through each recovery step and generate pre-filled letters, affidavits, and forms to send to credit bureaus, businesses, debt collectors, and IRS, as appropriate. The site’s advice can be customized to the consumer’s specific situation and can help consumers track their progress.

Identity Theft Insurance Covers a Limited Range of Expenses and Appears to Have Resulted in Few Claims

Identity theft services typically include identity theft insurance, which reimburses victims of identity theft for costs associated with the process of restoring their identity. Twenty-one of the 26 providers whose websites we reviewed indicated that they offered this insurance in their bundle of services. Identity theft insurance is a type of insurance policy typically offered through an identity theft service, although it is sometimes included as part of a homeowners insurance policy (or as a separate endorsement) or offered as a stand-alone policy for about \$25–\$50

annually, according to the Insurance Information Institute.³⁰ In 2015, insurers wrote approximately 17 million identity theft insurance policies as part of a package policy and about 500,000 stand-alone policies, according to the National Association of Insurance Commissioners.³¹ Representatives from an insurance company that is a market leader in identity theft insurance told us that in 2015 it covered between about 13 million and 15 million individuals through a plan that is offered through many large identity theft service providers.

The scope of items covered by identity theft insurance is generally limited. Identity theft insurance is limited in covering direct financial losses—that is, money that has been stolen. Instead, the insurance generally reimburses consumers for out-of-pocket expenses they incur related to the process of restoring their identity and restoring their credit records. The websites of 26 providers we reviewed indicated that most identity theft insurance policies offered an overall coverage limit of \$1 million. While individual policies varied, our review of policies offered through five identity theft services—including those that provided services for the OPM breaches—found that the reimbursement coverage was broadly similar. Most covered postage and notary fees; the cost of obtaining credit reports or implementing credit freezes; costs related to replacing documents such as driver's licenses and passports; travel costs and elder or child care expenses; lost wages (usually capped at \$4,000–\$7,500) associated with time or efforts spent resolving the identity theft; and attorney fees. All policies we reviewed covered limited direct financial losses related to stolen funds resulting from fraudulent electronic fund transfers, usually capped at limits ranging from \$10,000–\$50,000, although one provider had limits of \$100,000 and \$1 million for its premium products.

³⁰The Insurance Information Institute is an industry organization with the mission to improve the public's understanding of insurance.

³¹This policy information was collected through the *Cybersecurity and Identity Theft Insurance Coverage Supplement*, which all states require their multi-state insurers to file with the National Association of Insurance Commissioners. The mandatory data supplement is attached to insurers' annual financial reports, which requires all insurance carriers writing either identity theft insurance or cybersecurity insurance to report on their claims, premiums, losses, expenses, and in-force policies in these areas. The annual supplement was first required to be filed in April 2016 and included data for the year-ending 2015. The National Association of Insurance Commissioners is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia, and the five U.S. territories.

In practice, the value to consumers of identity theft insurance coverage may be limited. In large part this is because the process of resolving identity theft typically does not require significant expenses, according to many providers we spoke with and two consumer groups. The Bureau of Justice Statistics reported that in 2014, 5 percent of all identity theft victims reported indirect losses—defined as expenses such as legal fees, postage, notary fees, and other miscellaneous expenses—associated with their most recent incident of identity theft. Among those individuals reporting indirect losses of \$1 or more, the mean loss was \$261 and the median was \$10. In addition, the coverage for fraud involving wire transfers may be of limited value given that consumer liability for unauthorized charges is generally limited.

Information we collected indicates that both the number and dollar amounts of identity theft insurance claims have been low. We asked five major identity theft service providers, with millions of customers among them, and a major insurer for information about their insurance claims. The extent to which these companies provided us with claims information varied because some said it was proprietary. However, available information indicated few claims and small dollar amounts, appearing to rarely exceed a few thousand dollars:

- An insurance company that is a market leader in identity theft insurance did not provide its number of claims but told us that successful claims averaged about \$500–\$1,500 in reimbursed expenses per incident of identity theft, and its largest claim paid had been roughly \$50,000.
- One provider said it had experienced zero or “almost zero” claims in recent years.
- One provider did not provide the number or dollar amounts of claims, but said that its loss ratio (benefits paid out divided by premiums collected) was less than 2 percent.
- One provider told us that it had paid a total of 14 claims of more than \$1,000 each, the largest of which was \$9,350.
- A provider with a government contract covering more than 4 million people said that, as of April 2016, its insurance had paid out one claim, in the amount of \$1,519.
- One provider did not provide its number of claims but said that it had at least one claim of \$10,000.

Some identity theft service providers with whom we spoke acknowledged that identity theft insurance is of limited value to a consumer and that it was hard to imagine covered losses approaching the \$1 million limit. Two providers told us that the primary reason they provided identity theft insurance—and in an amount of \$1 million—was to stay competitive in the marketplace, given that such insurance has become a standard component of identity theft services. Two consumer groups have asserted that the insurance has other limitations—such as onerous requirements for filing a claim and exclusions for pre-existing identity theft—which further limits the policies’ value.

Some Types of Threats Are Typically Not Addressed by Existing Identity Theft Services

Identity theft services have evolved over the years. While originally they focused largely on credit monitoring, products now typically include identity monitoring services designed to detect other kinds of harm, as previously discussed. Nonetheless, existing products largely do not address many types of identity theft, including medical identity theft, identity theft refund fraud, synthetic identity theft, and other evolving threats.

Medical Identity Theft

Medical identity theft occurs when someone uses an individual’s name and personal identity to obtain medical services or prescription drugs fraudulently, including attempting to submit fraudulent insurance claims. The Ponemon Institute estimated that there were about 482,000 new cases of medical identity theft in the 12 months ending in November 2014.³² According to the Medical Identity Fraud Alliance—a public-private organization whose members include health care providers, government agencies, and academics—medical identity theft can create a financial burden on victims because they may be liable for reimbursing a health plan or provider for fraudulent use of services (in contrast to credit card or bank fraud, where consumer liability for such losses is generally limited). The Ponemon study found that 65 percent of medical identity theft victims said they incurred costs as a result of the theft, averaging about \$13,450. In addition, when a consumer’s medical information is used fraudulently by another person for medical treatment, incorrect information can appear in the victim’s personal medical records, which can result in misdiagnosis, incorrect treatment, or delays in receiving treatment.

³²Ponemon Institute LLC, *Fifth Annual Study on Medical Identity Theft* (2015). The Ponemon Institute is an independent research organization that focuses on privacy, data protection, and information security policy.

One of 26 identity theft services that we reviewed expressly addressed medical identity theft. That product works with the explanation-of-benefits delivery system of the user's health insurer to alert the user every time a claim is made against the user's health plan benefits.³³ Users can flag a claim as suspicious if, for example, they do not recognize the procedure or health care provider, and the company then will investigate the claim. The service is not offered directly to consumers; rather, it is offered as a benefit by health insurers to their members.

The remaining 25 (of the 26) identity theft services whose websites we reviewed did not indicate that they had products or services specifically to address medical identity theft. Some providers and an FTC staff person cited two significant challenges to addressing medical identity fraud with a consumer product. First, federal law restricts the ways in which companies can aggregate and share health information.³⁴ Second, health care data are highly compartmentalized, and there is no central repository or clearinghouse akin to the nationwide credit bureaus for health and health insurance information.

A 2013 report by the Medical Identity Fraud Alliance called for new products and services to be developed (or existing ones adapted) for protection of an individual's medical identity and early detection of medical identity theft.³⁵ The report noted that explanations of benefits do not effectively alert consumers to misuse of their benefits because they are not timely and are hard to read, and limited evidence exists that individuals report suspicious claims to their health plan. Most of the solutions to reducing medical identity theft that the alliance recommended did not rely on a consumer product but focused instead on efforts such as better verification of a patient's identity (such as through a smart medical card with chip technology) and detection of anomalies in claims indicating fraud. An FTC staff member told us he did not expect the solution to medical identity theft to lie in a direct-to-consumer product such as an

³³An explanation of benefits is a statement sent by a health insurance company to covered individuals that explains the medical services paid on the individual's behalf, as well as the date of the service and the amounts billed, covered, and paid.

³⁴The Health Insurance Portability and Accountability Act imposes restrictions on the use and disclosure of individually identifiable health information collected by covered health care entities. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

³⁵Gary R. Gordon, Ed.D, *The Growing Threat of Medical Identity Fraud: A Call to Action* (Medical Identity Fraud Alliance, July 2013).

identity theft service, but rather in a business-to-business product that helps health insurers and providers better identify fraudulent use.

Some identity theft services noted limited ways in which they address medical identity theft. For example, some identity monitoring services alert consumers if their medical insurance numbers are found on black-market websites. The websites of at least two providers state that they will help the customer request or review their explanation of benefits to help ensure that no one else is receiving treatment with their benefits. In addition, some providers told us that although they do not monitor health care information, their identity restoration service would assist with any restoration or financial recovery associated with medical identity theft.

Identity Theft Refund Fraud

Identity theft refund fraud occurs when an individual's Social Security number or other personally identifiable information is used to file a fraudulent tax return seeking a refund. IRS estimated that it paid at least \$2.2 billion in fraudulent calendar year 2015 refunds, and that it prevented at least \$12.3 billion more from going to fraudsters.³⁶ While identity theft refund fraud will not preclude legitimate taxpayers from receiving the refund they are due, the fraud can cause them hardship because authenticating their identities is likely to delay the processing of their actual returns and refunds.

No identity theft service expressly addresses identity theft refund fraud, according to our review of these services and interviews with representatives of providers, consumer groups, and federal agencies. Two stakeholders noted that third-party monitoring is not feasible because IRS cannot generally share taxpayer information.³⁷ As such, it is unlikely that there will be a direct-to-consumer product built around preventing identity theft refund fraud, according to an FTC staff member with whom we spoke. IRS recommends that consumers can protect themselves against identity theft by taking standard common sense measures to protect their Social Security number and other personally identifiable information (such as not carrying documents with their Social

³⁶Because of the difficulties in estimating the amount of undetectable fraud, the actual amount could differ from these estimates. For additional information, see GAO, *Identity Theft and Tax Fraud: IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program*, [GAO-16-508](#) (Washington, D.C.: May 24, 2016).

³⁷Federal law provides that returns and return information shall be confidential and prohibits officers and employees of the United States from disclosing any return or return information, subject to exceptions. See 26 U.S.C. § 6103.

Security number and only providing the number when required).³⁸ In addition, IRS can issue victims of identity theft refund fraud an Identity Protection Personal Identification Number to prevent future fraud.³⁹ Although no identity theft services seek to detect or prevent identity theft refund fraud, one provider told us that its service predicts the consumer's risk for becoming a victim of refund fraud and provides education on steps they can take to detect or prevent it, such as filing one's tax return early. Others note that their identity restoration services can provide guidance to consumers who become victims of identity theft refund fraud.

Other Threats

Criminals can use stolen personal information for a variety of other objectives as well, and existing identity theft services generally have limited value in addressing these threats.

Government benefits fraud. Identity thieves can use stolen personal information to fraudulently obtain government benefits. For example, the Social Security Administration has reported that personal information of Social Security beneficiaries has been used to fraudulently redirect the beneficiary's direct deposit benefits. In addition, the Department of Labor has reported that identity thieves have used stolen personal information to file multiple fraudulent claims for unemployment insurance benefits. The cost of these crimes is typically borne by the government and the

³⁸IRS provides guidance to taxpayers related to identity theft on its website, including contact information and steps for victims of identity theft refund fraud. For example, victims can complete the IRS Form 14039, Identity Theft Affidavit, if their electronically filed tax return is rejected because of a duplicate filing. The guidance is available at <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft>.

³⁹Identity Protection Personal Identification Numbers help prevent future identity theft refund fraud because, once issued, the number must accompany the taxpayer's electronically-filed tax return or else IRS will reject the return. If a paper return has a missing or incorrect personal identification number, IRS delays processing the return while the agency determines if it was filed by the legitimate taxpayer. See GAO, *Identity Theft: Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*, [GAO-14-633](#) (Washington, D.C.: Aug. 20, 2014).

taxpayer.⁴⁰ However, the crimes can have adverse effects on the victims as well, including delays in receiving benefits and time spent resolving the problem. Identity theft restoration and insurance services can help the consumer reduce the time spent to resolve these issues and cover related expenses, but identity theft services are generally not designed to detect government benefits fraud. One company that provides identity theft services said it also has a separate division that uses unemployment databases to alert state unemployment agencies of suspected false claims filed against its corporate clients and their workers.

State-sponsored espionage. Nations use cyber tools as part of their information-gathering and espionage activities. For example, according to a House committee report, some security experts have cited evidence that a foreign government likely played a role in the theft of OPM's personnel files and security clearance background investigation information on millions of individuals.⁴¹ An FTC staff member noted that when the source of the data breach appears to be a nation-state (as opposed to a private party), the risk of the information being sold for monetary purposes is likely to be lower, but credit and identity monitoring may be necessary because the risk of identity theft is still present. A security expert noted that no one knows where stolen data will end up and that even a nation-state could sell it. Two providers, a security expert, and a consumer organization told us they believed that the type of information stolen—rather than the source of the breach—generally should determine what services to provide. However, several providers noted that cases where a nation-state appears to be the hacker might require different decisions on the features and length of time that services are offered. One noted that nation-state actors can wait much longer to

⁴⁰To help federal program managers combat fraud and preserve integrity in government agencies and programs, GAO identified leading practices for managing fraud risks. See GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 2015). Furthermore, the Fraud Reduction and Data Analytics Act of 2015 requires, among other things, the Office of Management and Budget (OMB) to, in consultation with the Comptroller General, establish guidelines for federal agencies to establish financial and administrative controls to identify and assess fraud risks and design and implement control activities in order to prevent, detect, and respond to fraud, including improper payments. The guidelines OMB establishes must incorporate the leading practices identified in GAO's Fraud Risk Framework. Pub. L. No. 114-186, § 3, 130 Stat. 546, 546 (2016).

⁴¹House of Representatives, Committee on Oversight and Government Reform, 114th Congress, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation* (Washington, D.C.: Sept. 7, 2016).

use compromised information and therefore it may make sense to provide a longer period of coverage to individuals in these cases.

Reputational and emotional harm and loss of privacy. The harms caused by a data breach can extend beyond tangible financial loss to include emotional distress, a loss of privacy, or harm to one's reputation. The House Committee report on the OPM data breaches noted that the information stolen from background investigations included some of the most intimate and potentially embarrassing aspects of a person's life, such as the person's mental health history, misuse of alcohol or drugs, or problems with gambling. The Department of Justice's 2014 survey of identity victims found that about 21 percent of those who experienced identity theft of personal information reported suffering severe emotional distress.⁴² The identity theft services we reviewed generally do not expressly address these types of harm, although credit and identity monitoring alerts could indicate the specific type of personal information that was stolen. One company told us it was evaluating how to incorporate monitoring of social media into its services given that a hacked social media account can, among other harms, cause embarrassment or affect one's reputation.

Synthetic identity theft. Synthetic identity theft—which the federal government has identified as an emerging trend—involves the creation of a fictitious identity, typically by using a combination of real data from multiple individuals and fabricated information.⁴³ For example, an identity thief may use one person's Social Security number and combine it with a fictitious name and another person's address to create a new identity that may be used to apply for credit or other fraudulent activities. Credit monitoring services do not typically detect new-account fraud using a synthetic identity, according to a security expert with whom we spoke, because credit reports do not reveal all credit history entries connected to a Social Security number; instead, only entries appear that exactly match a consumer's name, Social Security number, and other personal information. Accounts that are opened using the consumer's Social Security number but a different name would appear at a credit bureau as

⁴²Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* (Washington, D.C.: September 2015).

⁴³GAO has work under way on synthetic identity theft and expects to issue a report in 2017.

a “sub-file”—a file linked to a consumer’s main credit file that would typically not be included on the consumer’s credit report.

Losses resulting from synthetic identity theft often are borne by the affected financial institutions rather than the individuals whose identifying information was used to help create the fake identity, according to security experts. However, an individual may experience problems if the new identity eventually tracks back to the victim’s credit or tax records—for example, a creditor conducting a full background check would see all of the accounts linked to the applicant’s Social Security number, including the fraudulent sub-files. Synthetic identity theft can harm minors in particular because the illicit use of their Social Security number can damage their ability to apply for credit when they turn 18. Some providers told us their identity monitoring services can detect potential synthetic identity theft of minors since any detection of a minor’s Social Security number is considered a red flag because minors typically don’t have credit activity.

Various Parties Collect Information on Identity Theft Services, but Services’ Effectiveness Has Not Been Evaluated

Various parties have collected and analyzed information on the products advertised and delivered by providers of identity theft services. However, we did not identify any federal agency or private-sector entity that has formally assessed whether offering these services after a data breach is an effective way of delivering intended outcomes, such as mitigating specific risks or reassuring affected individuals. The lack of data on outcomes produced by the services may be one of the significant challenges to conducting such an assessment.

While we did not identify evaluations of the effectiveness of identity theft services, we did find that some service providers, entities that purchase services, and third-party research and advocacy organizations have collected and analyzed information about the quality of individual providers’ services:

- **Service providers.** Several identity theft service providers told us that they track quality metrics, including scores on customer surveys, customer retention rates, and the time it takes—as well as the success rate—to resolve fraudulent accounts and records on

customers' behalf.⁴⁴ Some providers also told us they collect information on the number of "hits" their identity monitoring detects on sources such as black-market websites.

- **Entities that purchase services.** Federal and private-sector entities that purchase identity theft services in response to a data breach told us that they receive information from the providers about the take-up rate (the percentage of people offered free services who enroll), and that they monitor how quickly and effectively the providers respond to inquiries or concerns.⁴⁵ The federal contracts awarded in 2015 for the OPM breaches provide for federal agencies to receive somewhat more extensive information about the services delivered by contractors, such as information about call-center wait times and the number and status of identity restoration cases.
- **Research and advocacy organizations.** Third-party research organizations, such as Javelin Strategy & Research and Forrester Research, collect and analyze certain aspects of identity theft service providers, including the features of the products they offer, their experience responding to large-scale breaches, and the subject-matter expertise of their key personnel. In addition, as discussed later in this report, the Consumer Federation of America has reviewed providers' websites and reported on the clearness and completeness of the information they provide.

Staff from some federal agencies we spoke with told us they would face significant challenges to conducting such an evaluation, including the limited amount of data available on federal use of these services. In particular, one federal official stated that the data needed to assess a provider's performance under a specific contract differ from the data needed to assess whether providing identity theft services after a breach is an effective way of producing intended outcomes. The confidentiality of personal data associated with the products could also be a limiting factor in trying to evaluate their effectiveness.

⁴⁴Two providers we spoke with told us that their retention rates—the percentage of people that signed up for the services for 1 year or more—were about 70 percent and 85 percent, respectively.

⁴⁵According to federal and private entities with whom we spoke, the rate at which consumers enrolled in free identity theft services offered in response to a breach typically ranged from 3 percent to 25 percent. In some cases, the identity restoration and insurance components of these services are available to consumers whether or not they enroll.

Consumer Complaints and Enforcement Actions Have Focused on Billing and Marketing Issues among Some Providers

Consumer complaints about identity theft services have largely been related to billing issues, according to our review of federal complaint data. At least 16 federal enforcement actions have been taken related to the marketing, billing, and other practices of identity theft services—seven against service providers themselves and nine against banks offering them in conjunction with a credit card. Identity theft services collect and retain a broad range of customers’ sensitive personal information. Our review of services’ websites found most were generally clear and comprehensive, but we also found examples of information presented that could be construed as misleading or vague.

Consumer Complaints Have Generally Focused on Billing and Account Issues

There were an estimated 2,500 consumer complaints related to identity theft services in 2015, according to our analysis of FTC’s Consumer Sentinel Network and CFPB’s Consumer Complaint Database.⁴⁶ To determine the nature of those complaints, we reviewed the narrative associated with complaints, as available, and CFPB’s subcategories for complaints related to identity theft services in CFPB’s Consumer Complaint Database from December 2011 to June 2016.⁴⁷ We found that about 89 percent of the complaints were about billing issues, mostly centered on problems related to cancelling the service or being enrolled in a service without the consumer’s knowledge or permission. The remaining complaints—approximately 11 percent—were complaints about other issues, such as unhelpful customer service, not receiving alerts about changes in a credit report, and unwanted marketing or sales pressure. In addition, we reviewed complaints related to identity theft services received by the Better Business Bureaus from April 2013 to April

⁴⁶FTC’s Consumer Sentinel Network is a database of consumer complaints received by FTC, as well as those filed with certain other federal and state agencies and nongovernmental organizations, including CFPB and the Better Business Bureaus. CFPB collects and aggregates consumer complaints about financial products and services and provides complaints and related data in its Consumer Complaint Database. For the purposes of our review, we asked FTC staff to conduct a search of the Consumer Sentinel Network using the terms “credit monitoring,” “identity protection,” “identity theft protection,” “ID protection,” and “ID theft protection.” This search resulted in 3,000 complaints, but our review of CFPB complaint data using the agency’s issue and subissue area categorizations indicated that about 500 of these were complaints related to fraud alerts rather than complaints about identity theft services.

⁴⁷We reviewed complaint narratives related to identity theft services from CFPB’s database but not from other sources included in FTC’s Consumer Sentinel Network database because those other sources do not make the narrative available.

2016. The bureaus assign complaints to categories, and the single largest category, with 33 percent, was related to billing and unauthorized charges. The second most common category, with 13 percent, related to service quality.

However, in general, consumer complaint data have limitations and may not be a reliable indicator of the extent of problems. For example, not all consumers who experience problems may file a complaint, and not all complaints are necessarily legitimate or categorized appropriately. In addition, a consumer could submit a complaint more than once, or to more than one entity, potentially resulting in duplicate complaints.

Enforcement Actions Related to Identity Theft Services Have Been Taken Against Providers and Several Banks

At least 16 federal enforcement actions related to the marketing, billing, and other practices of identity theft services had been taken as of September 2016. Seven of these actions were taken against providers of identity theft services—LifeLock (2 actions), TransUnion, Affinion, Intersections, and Consumerinfo.com/Experian (2 actions). The other 9 enforcement actions were taken against financial institutions that offer identity theft services as additional, optional services in conjunction with a credit card, often referred to as credit card add-on products.

- **LifeLock.** In March 2010, FTC and 35 state attorneys general announced a settlement with LifeLock, Inc., after charges that the company used false claims to promote its identity theft services. FTC’s complaint alleged that since 2006, LifeLock’s advertisements had misrepresented that the company’s products would prevent identity theft and constantly monitored activity on customer credit reports. FTC’s complaint also alleged that LifeLock made false claims about its data security, such as that the personal data it held were encrypted and shared only on a need-to-know basis. Without admitting FTC’s allegations, LifeLock agreed to change its practices and pay \$11 million to FTC and \$1 million to the group of 35 state attorneys general. In December 2015, FTC and LifeLock settled charges that the company violated the 2010 court order by continuing to make false claims about its identity theft services and by failing to take steps required to protect its users’ data. LifeLock, without admitting or denying the allegations, agreed to pay \$100 million to settle these charges.
- **TransUnion.** In January 2017, CFPB took action against TransUnion after alleging that, among other things, it used false promises to lure consumers into costly recurring payments for credit-related products, which included credit monitoring and other identity theft services.

CFPB alleged that the company deceived consumers by automatically enrolling them in subscription programs for credit-related products after falsely claiming they cost \$1. Under the consent order, TransUnion, while neither admitting nor denying CFPB's allegations, agreed to pay about \$13.9 million in restitution to affected consumers and \$3 million in civil money penalties, and to modify its practices. Under the consent order, TransUnion neither admitted nor denied CFPB's allegations.

- **Affinion.** In July 2015, CFPB filed a complaint against Affinion Group Holdings and several affiliated companies (Affinion), which sold identity theft protection services by establishing marketing and service agreements with banks. The complaint alleged that from about July 2010 through August 2012, Affinion billed full product fees to at least 73,000 consumer accounts while failing to provide the full credit monitoring or credit report retrieval services promised and failed to refund fees to those consumers. The complaint also alleged that Affinion telephone representatives frequently misled consumers about product benefits. Under the consent order between CFPB and Affinion, the company, while neither admitting nor denying CFPB's allegations, agreed to change its billing and retention practices and pay about \$6.76 million in monetary relief for eligible consumers and \$1.9 million in civil money penalties.
- **Intersections.** CFPB filed a complaint in July 2015 against the identity theft service provider Intersections Inc., alleging that the company billed or instructed banks to bill approximately 300,000 consumers who signed up for their products even though the company could not provide the credit monitoring or other benefits for various reasons (such as failing to obtain a valid authorization from the consumer or having incomplete Social Security information). In settling the case, Intersections, while neither admitting nor denying CFPB's allegations, agreed to end its unfair billing practices, reimburse consumers approximately \$55,000, and pay a \$1.2 million civil money penalty.
- **Consumerinfo.com/Experian.** In August 2005, FTC announced that it had reached a settlement with the identity theft service provider Consumerinfo.com, Inc., doing business as Experian Consumer Direct. FTC alleged that the company had deceptively marketed "free credit reports" by not adequately disclosing that consumers automatically would be signed up and charged for a credit monitoring service if they did not cancel within 30 days. The settlement required consumer redress and a \$950,000 disgorgement payment to FTC. In February 2007, FTC reached a second settlement with the company

after alleging it had violated the previous settlement, requiring it to give up \$300,000 in ill-gotten gains and barring it from further misrepresentation.

- **Financial institutions.** Since 2012, enforcement actions have been taken against at least nine financial institutions for their marketing and billing practices related to identity theft services.⁴⁸ The federal agencies that have taken these actions, sometimes jointly, have included CFPB, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation. The financial institutions in these cases were not themselves providing identity theft services but were selling them as an add-on to a credit card or other financial product. While the specific allegations varied, they typically involved engaging in deceptive marketing and sales tactics or billing consumers for products they did not receive. In each case, the firms agreed to change their practices and pay consumer redress, a civil money penalty, or both.

Identity Theft Services Typically Collect and Hold a Broad Range of Sensitive Personal Information

Identity theft services collect and retain a broad range of customers' sensitive personal information. At a minimum, this information generally includes name, address, Social Security number, and other information required to enroll in credit monitoring. However, to conduct identity monitoring services, companies also may collect and retain information from customers' credit card and bank accounts, passports, driver's licenses, and medical insurance cards, as well as e-mail addresses and phone numbers. Because data breaches have become so prevalent, some parties have expressed concerns that the array of personal information held by identity theft services could put their customers at risk in the event of a cyberattack.

Underscoring these concerns are FTC's 2010 and 2015 enforcement actions against LifeLock, which, as noted earlier, alleged that the company failed to provide reasonable and appropriate security measures. Among other things, allegations included a failure to use good password practices, limit access to personal information to employees on a need-to-know basis, install patches and critical updates on its network, and install antivirus or antispyware programs on computers used by employees to remotely access the network. The company did not admit to these

⁴⁸The financial institutions involved in the enforcement actions include American Express Bank, Bank of America, Capital One Bank, Chase Bank, Citibank, Discover Bank, First National Bank of Omaha, U.S. Bank, and Wells Fargo Bank.

allegations in its settlements with FTC, but representatives of LifeLock said that the company had taken many steps since then to achieve the highest security standards in the industry.

One representative of the identity theft services industry acknowledged there were data security risks associated with having a single company possess so much personal and financial information about an individual. In the Securities and Exchange Commission (Form 10-K) filings we reviewed of five companies that provide identity theft services, the companies reported collecting and storing significant amounts of confidential information, including personally identifiable information, credit card information, and other critical data, and all identified data breaches and other information security concerns as a significant risk and potential vulnerability.⁴⁹ In their filings, all five companies also asserted that they had robust security programs to address these vulnerabilities. Staff at FTC and CFPB told us that, as a whole, the identity theft services industry may not necessarily represent more of a security risk than other industries that collect and retain sensitive personal information, such as health care organizations. In addition, companies in industries other than identity theft services that aggregate large amounts of sensitive personal information—such as credit bureaus—have experienced large-scale breaches of sensitive data in recent years.

Certain federal laws and regulations that govern the sharing and protection of personal information, and that prohibit unfair or deceptive acts or practices, may be applicable to identity theft services and the companies that offer them, depending on the circumstances. These include the Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Credit Repair Organizations Act, Federal Trade Commission Act, and the Consumer Financial Protection Act of 2010. (See app. II for additional information about these statutes.)

⁴⁹Federal securities laws require public companies to disclose information on an ongoing basis. These disclosures include annual reports on Form 10-K, which provides a comprehensive overview of the company's business and financial condition and includes audited financial statements.

Many Identity Theft Services' Websites Are Generally Clear and Comprehensive, but Some Appear Misleading or Vague

Although the websites of many identity theft services generally provide clear and comprehensive descriptions of the services, we found some examples where the information seems misleading or vague. In 2009, the Consumer Federation of America conducted a study of the websites of 16 identity theft service providers and said that generally it found the descriptions of the services to be confusing, unclear, and ambiguous.⁵⁰ In particular, the study reported that the websites often failed to provide clear, complete information about what the provider did and how the services worked; did not always clearly disclose costs; suggested the service offered more protection against identity theft than it could actually provide; and provided few details about the insurance coverage the provider offered. Subsequent to its report, the Consumer Federation of America formed a working group consisting of at least 12 companies that provide identity theft services and several consumer groups. The working group developed a set of best practices designed to encourage identity theft services to provide clear, complete information about their services and to discourage unfair and deceptive practices.⁵¹ In 2012, the Consumer Federation of America published a study of companies' compliance with these best practices. The study found that the majority of websites met most of the best practices fairly well, although on some websites it still identified overstatement of benefits and lack of transparency.⁵²

In August 2016, we conducted our own review of the websites of 10 identity theft services.⁵³ In general, most of the websites provided reasonably clear and comprehensive descriptions of the services provided. However, we also identified examples on some of the websites where the information seemed to be misleading or vague:

⁵⁰Consumer Federation of America, *To Catch a Thief: Are Identity Theft Services Worth the Cost?* (Washington, D.C.: March 2009).

⁵¹Consumer Federation of America, *Best Practices for Identity Theft Services* (Washington, D.C.: Mar. 10, 2011). A revised version was published in November 2015. Consumer Federation of America, *Best Practices for Identity Theft Services, Version 2.0* (Washington, D.C.: Nov. 17, 2015).

⁵²Consumer Federation of America, *Best Practices for Identity Theft Services: How Are Services Measuring Up?* (Washington, D.C.: Apr. 18, 2012).

⁵³The 10 websites we reviewed were selected to represent a mix that included some of the industry's largest participants, as well as some smaller ones. Our review was designed to provide illustrative examples and was not a generalizable sample.

-
- Providers sometimes used language that appeared to incorrectly imply that credit monitoring prevents—rather than just detects—identity theft. For example, one stated “The best identity theft protection...help[s] prevent identity theft before it happens. With [provider], you get great credit protection features, including credit monitoring and alerts.” Another described credit monitoring as “credit card protection.”
 - Some websites cited statistics about identity theft that could be misleading. For example, websites stated that “1 in 4 People have Experienced Identity Theft,” “11 million identities are stolen each year,” and “Nearly 10 million Americans have their identities stolen each year.” These figures include existing-account fraud—such as misuse of credit card numbers—which the service being advertised was not designed to detect. Similarly, one website included a marketing video in which a woman describes fraudulent charges on her father’s credit card bill, even though the service would not alert a customer to such charges.
 - While descriptions of most services were generally comprehensive, in some instances they appeared to be vague or incomplete. One website provided very little information on its home page about what the service actually did, with additional information available only through an inconspicuous link that was difficult to locate. The description of identity restoration on another website conveyed little more than that a protection specialist was available by telephone. On a third website, the price of the service was difficult to access and appeared to be available only if one began the enrollment process.

Various Factors Affect Decision Making about Offering Identity Theft Services, and Federal Guidance Could Be Improved

In the federal sector, although several agencies have specific requirements related to the provision of identity theft services, there is no general requirement for all agencies to provide identity theft services after data breaches. However, certain laws and policies guide agencies’ decisions about offering these services, including general guidance from the Office of Management and Budget (OMB) and agencies’ own policies. Federal law requires OPM to offer identity protection coverage, including identity theft insurance, to those affected by the breaches it announced in 2015, but we found that the required insurance coverage of \$5 million may be too high. In addition, OPM did not have policies in place and did not document its decision making on offering services after its two 2015 breaches, and the agency offered duplicative services to some individuals affected by both breaches. In the private sector, companies may offer affected consumers identity theft services for reasons independent of the effectiveness of the services, such as to avoid liability.

At Least Two Agencies Are Required to Provide Services, and the Amount of Insurance Coverage That OPM Is Required to Provide May Be Unnecessarily High

No federal law specifically requires all agencies to provide identity theft services to individuals affected by a breach. However, at least two agencies—the Department of Veterans Affairs (VA) and OPM—are required by statute to provide these services in certain circumstances. The Veterans Benefits, Health Care, and Information Technology Act of 2006 requires VA to provide identity theft services after a data breach under certain circumstances.⁵⁴ The Consolidated Appropriations Act, 2016, requires OPM to provide identity theft services to individuals whose Social Security numbers were compromised during the data breach of personnel records that was announced on June 4, 2015, or the data breach of OPM systems containing information from the background investigations of current, former, and prospective federal employees and of other individuals.⁵⁵

One of the requirements for OPM included in the Consolidated Appropriations Act, 2016, is that OPM provide individuals affected by the data breaches it announced in 2015 with not less than \$5 million in identity theft insurance for a period of not less than 10 years (through at least Dec. 18, 2025).⁵⁶ Prior to the passage of the Consolidated Appropriations Act, 2016, the services OPM offered to those affected by the breaches included \$1 million in insurance coverage. As discussed earlier, many identity theft service providers with whom we spoke acknowledged that identity theft insurance is of limited value to a consumer and that it was hard to imagine covered losses approaching the

⁵⁴Pub. L. No. 109-461, § 902(a), 120 Stat. 3403, 3455 (2006) (codified at 38 U.S.C. § 5724(a)(2)). Specifically, if the Secretary of Veterans Affairs determines, based on the findings of a required risk analysis, that a reasonable risk exists for the potential misuse of sensitive personal information involved in a data breach, the Secretary is required to provide “credit protection services” in accordance with regulations. VA regulations provide that where such a reasonable risk exists, the Secretary may offer one or more of the following: (1) one year of credit monitoring services consisting of automatic daily monitoring of at least three relevant credit bureau reports; (2) data breach analysis; (3) fraud resolution services, including writing dispute letters and initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution; and/or (4) one year of identity theft insurance with \$20,000 coverage at \$0 deductible. 38 C.F.R. § 75.118(a).

⁵⁵Pub. L. No. 114-113, § 632, 129 Stat. 2242, 2470 (2015). The statute requires OPM to provide complimentary identity protection coverage that is not less comprehensive than the complimentary identity protection coverage that OPM provided to affected individuals before the date of the act. This coverage must be effective for a period of not less than 10 years and must include not less than \$5 million in identity theft insurance.

⁵⁶*Id.*

\$1 million limit. Nearly all the providers with whom we spoke said that it was not necessary to increase the insurance coverage beyond \$1 million. Representatives from an insurance company that is a market leader in identity theft insurance told us that while a claim beyond \$1 million was theoretically possible—for example, if a case involved high legal fees and fraudulent electronic funds transfer—coverage in excess of \$1 million was unnecessary.

The additional cost to the government of providing \$5 million in insurance coverage does not appear to be substantial. According to OPM, the two contracts awarded in 2015 for identity theft services for individuals affected by the OPM data breaches were modified to increase insurance coverage from \$1 million to \$5 million, but these modifications resulted in no additional cost to the government. Subsequently, as of February 2017, all three of the contractors on the Identity Protection Services Multiple Award Blanket Purchase Agreement have made updates to include \$5 million in insurance coverage, without increasing their prices as a result of this change. One of these contractors told us it factored insurance coverage into the overall costs of the contract. It declined to estimate the additional cost of providing \$5 million versus \$1 million in insurance coverage, but noted the additional costs it faced were mostly administrative, given that claims have been so low.

Any resulting future costs that may result from the increase in insurance coverage to \$5 million may not be aligned with goals identified by both Congress and the administration to reduce unnecessary spending, given that there does not seem to be a corresponding benefit to such coverage.⁵⁷ In addition, the high dollar amount of the required insurance coverage might give consumers the impression that the insurance coverage is broad when the scope of items covered by identity theft insurance is generally limited to out-of-pocket expenses that are typically modest. Furthermore, according to representatives from a market leader in providing identity theft insurance, there is a risk that the required increase in insurance coverage could drive up the industry standard for

⁵⁷For example, see Executive Office of the President, *Building a 21st Century Government by Cutting Duplication, Fragmentation, and Waste* (Washington, D.C.: Feb. 28, 2012). In addition, in 2010, Congress included a provision in statute for GAO to identify federal programs, agencies, offices, and initiatives with duplicative goals and activities within departments and government-wide, and report to Congress annually on the findings. Statutory Pay-As-You-Go Act of 2010, Pub. L. No. 111-139, § 21, 124 Stat. 8, 29 (2010).

the amount of insurance coverage that identity theft services provide with little additional benefit to the consumer.

OMB Policy Governs Agencies' Responses to Data Breaches, but Its Guidance to Agencies Does Not Address Services' Effectiveness

Although federal law does not generally require agencies to offer identity theft services, it does require agencies to make plans for responding to data breaches. Under the Federal Information Security Modernization Act of 2014 (FISMA), agencies must develop, document, and implement an agency-wide security program that includes, among other things, procedures for detecting, reporting, and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done.⁵⁸ FISMA requires the Secretary of Homeland Security, in consultation with the Director of OMB, to assist with, among other things, overseeing and monitoring agencies' implementation of security requirements, and to provide operational and technical assistance to agencies in implementing information security policies.⁵⁹ The information security program that agencies are required under FISMA to develop, document, and implement also must include notifying and consulting with the federal information security incident center about security incidents. The U.S. Computer Emergency Readiness Team, a component of the Department of Homeland Security (DHS), operates this center. FISMA also requires OMB to oversee agency information security policies and to ensure that data breach notification policies and guidelines are updated periodically.⁶⁰

In January 2017, OMB issued a policy memorandum to provide guidance for federal agencies to prepare for and respond to breaches of personally

⁵⁸See Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 2(a), 128 Stat. 3073, 3080 (2014) (codified as amended at 44 U.S.C. § 3554(b)).

⁵⁹This assistance includes operating the federal information security incident center and—upon request by an agency—deploying, operating, and maintaining technology to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities.

⁶⁰Pub. L. No. 113-283, § 2(a), (d), 128 Stat. 3073, 3075, 3085 (codified as amended at 44 U.S.C. § 3553(a) and note).

identifiable information.⁶¹ This memorandum does not set a specific threshold or describe criteria for when agencies should provide identity theft services to individuals, but it instructs agencies to select services based on the risks of harm resulting from a particular breach.⁶² It notes that the services available in today's marketplace mitigate risks only of financial identity theft and do not mitigate potential harms resulting from evolving threats, such as medical identity theft or government benefits fraud. The memorandum states that if no service would mitigate a specific risk of harm, the agency may choose not to provide identity theft services to potentially affected individuals. This memorandum also describes different types of identity theft services—credit monitoring, identity monitoring, identity restoration, and insurance—and some of their benefits and limitations, and it includes a brief description of what the services do not cover and other important factors for consideration.

OMB's 2017 memorandum also includes actions other than identity theft services that agencies can consider taking to mitigate the risk of harm to affected individuals. For example, it cites potential countermeasures, such as proactively notifying banks when credit card information has been compromised, and requiring users to change passwords when they have been compromised. In addition, it instructs agencies to consider what guidance to provide to those individuals about steps they may take to mitigate their own risk of harm—such as requesting fraud alerts or credit freezes, changing or closing accounts, and taking advantage of guidance available from FTC. The memorandum states that it seeks to provide agencies with the flexibility to tailor their response to a breach based

⁶¹Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, *Preparing for and Responding to a Breach of Personally Identifiable Information*, M-17-12 (January 3, 2017). In this memorandum, OMB defines personally identifiable information as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. OMB was directed to update this guidance by the October 2015 Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government, Office of Management and Budget, Memorandum for the Heads of Departments and Agencies, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, M-16-04 (Oct. 30, 2015).

⁶²The 2017 guidance superseded guidance previously issued in 2006. Office of Management and Budget, Memorandum for the Heads of Departments and Agencies, *Recommendations for Identity Theft Related Data Breach Notification* (Sept. 20, 2006). For additional information about that guidance, see GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, [GAO-14-34](#) (Washington, D.C.: Dec. 9, 2013) and *Privacy: Lessons Learned about Data Breach Notification*, [GAO-07-657](#) (Washington, D.C.: Apr. 30, 2007).

upon the specific facts and circumstances of each breach and the analysis of the risk of harm to potentially affected individuals.

However, the 2017 guidance memorandum does not address the effectiveness of identity theft services relative to lower-cost alternatives. For example, while the guidance advises agencies on the circumstances in which identity theft services may or may not be most appropriate, it does not speak to the issue of whether these services are preferable to alternatives or countermeasures, such as fraud alerts, credit freezes, or the agency conducting its own monitoring of databases related to compromised data. As a result, the guidance may not fully reflect the most useful and cost-effective options agencies should consider in response to a breach. This may not be consistent with OMB's circular on risk management and internal controls in the federal government, which states that federal leaders and managers are responsible for implementing management practices that effectively respond to risks to improve effectiveness and efficiency.⁶³

OMB and GSA have taken steps aimed at streamlining the process of purchasing identity theft services for federal agencies. In 2006, GSA issued a government-wide multiple award Credit Monitoring Blanket Purchase Agreement.⁶⁴ In a 2006 memorandum, OMB instructed agencies to review the blanket purchase agreements when new requirements for credit monitoring services arise and to inform GSA and OMB when purchasing credit monitoring services other than through these agreements.⁶⁵ In 2015, GSA replaced the 2006 multiple award agreement, which had expired, and issued the new Identity Protection Services Multiple Award Blanket Purchase Agreement. According to GSA, the requirements for these blanket purchase agreements were changed after the discovery of the first 2015 OPM breach to require providers to have more stringent information technology security protections. In 2016, OMB issued a memorandum requiring agencies to

⁶³Office of Management and Budget, Memorandum to the Heads of Departments and Agencies, *Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular No. A-123, M-16-17 (July 15, 2016).

⁶⁴As noted previously, a blanket purchase agreement is a simplified method of filling anticipated repetitive needs for supplies or services by establishing charge accounts with qualified sources of supply. 48 C.F.R. § 13.303-1(a).

⁶⁵Office of Management and Budget, Memorandum for the Heads of Departments and Agencies, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)*, M-07-04 (Dec. 22, 2006).

use the GSA Identity Protection Services Multiple Award Blanket Purchase Agreement when purchasing these services, with limited exceptions.⁶⁶ In addition, in 2015 and 2016, OMB and DHS instructed agencies to have contracts for identity theft services in place, or to be ready to establish such contracts quickly in the event of a data breach.⁶⁷

Several Federal Agencies Have Their Own Policies on Offering Identity Theft Services

In addition to OMB's general guidance, several agencies have policies that specify when to offer identity theft services.⁶⁸ For example, DHS's policy restates the guidance provided in OMB's 2006 memorandum on data-breach response and allows DHS components to decide whether or not to offer credit monitoring services after breaches.⁶⁹ It states that DHS components should consider the seriousness of the risk of identity theft resulting from a breach and the cost of the services when deciding whether to offer credit monitoring to affected individuals. VA's policy provides more detailed guidance, including which types of breached information do and do not warrant offers of identity theft services.⁷⁰ For example, the guidance states that if a breach exposes an individual's full name, with no other identifying information, identity theft services are not

⁶⁶Office of Management and Budget, Memorandum for the Heads of Departments and Agencies, *Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response*, M-16-14 (July 1, 2016).

⁶⁷FISMA requires agencies to report annually on the adequacy and effectiveness of their information security policies, procedures, and practices. 44 U.S.C. § 3554(c)(1). OMB and DHS issued FISMA performance metrics for agencies in October 2015 and October 2016. Both sets of metrics require that agencies either (1) have contracts for identity theft services in place or (2) have assessed the scope, cost, and time to execute such a contract. The metrics documents identify this requirement as one of the metrics related to breach recovery, which the documents define as the restoration of capabilities impaired by a cybersecurity event. The metrics documents refer agencies to the blanket purchase agreements as a resource for establishing an agreement for identity theft services. Office of Management and Budget and Department of Homeland Security, *FY 2017 CIO FISMA Metrics*, Version 1.00 (Oct. 1, 2016); and Office of Management and Budget and Department of Homeland Security, *FY 2016 CIO FISMA Metrics*, Version 1.00 (Oct. 1, 2015).

⁶⁸In a 2013 report that evaluated data-breach response at eight federal agencies, we found that seven of these eight agencies had policies and procedures in place to determine whether services such as credit monitoring should be offered to affected individuals. [GAO-14-34](#), 11.

⁶⁹Department of Homeland Security, *Privacy Incident Handling Guidance* (Jan. 26, 2012).

⁷⁰Department of Veterans Affairs, *Handbook 6500.2: Management of Breaches Involving Sensitive Personal Information* (Washington, D.C.: July 28, 2016).

warranted. If a full name and date of birth are exposed, identity theft services are warranted, according to the guidance.

Some agencies decide in advance of a breach on a standard package of services to offer affected individuals. For example, IRS's *Internal Revenue Manual*—the primary, official source of instructions to IRS staff on the administration and operation of IRS—specifies a package of services that includes three-bureau credit monitoring and identity theft insurance but not restoration services or identity monitoring.⁷¹ VA's regulations provide that the Secretary of Veterans Affairs may offer, as warranted, three-bureau credit monitoring, data-breach analysis, fraud resolution services, identity theft insurance, or a combination of these services, but the regulations do not specifically mention identity monitoring.⁷² These agency policies sometimes specify the duration of the services. For example, IRS and VA policies both provide for the offering of 1 year of credit monitoring. VA officials told us that under the agency's policy, it cannot offer services for a period longer than 1 year. In some cases, agencies proactively award a contract for a predetermined package of identity theft services to be used in the event of a breach. For example, the U.S. Postal Service awarded such a contract in 2013 and subsequently used it to purchase services for more than 800,000 individuals affected by a 2014 data breach.

OPM Does Not Have a Policy on When to Offer Identity Theft Services and Lacks Documentation of Its Decision Making

After the breaches of personnel records and background investigations data were discovered in 2015, OPM made decisions about offering identity theft services without established OPM policy or standards. Unlike some agencies, OPM's breach-response policies and procedures do not specifically address identity theft services. These documents address other aspects of breach response, such as assessing whether a breach led to data loss, but do not address whether and when to offer identity theft services, and do not establish a standard package of these services.⁷³ As a result, OPM officials had to make a number of key

⁷¹Internal Revenue Service, *Internal Revenue Manual*, Part 10, Chapter 5, Section 4, accessed September 7, 2016, https://www.irs.gov/irm/part10/irm_10-005-004.html.

⁷²See 38 C.F.R. § 75.118(a).

⁷³Office of Personnel Management, *Cyber Protection & Defense Manual* (Washington, D.C.: February 2016); *Information Security and Privacy Policy* (Washington, D.C.: Mar. 31, 2011); *Information Security and Privacy Policy Addendum* (Washington, D.C.: March 2012); and *Information Security and Privacy Policy Addendum* (Washington, D.C.: February 2013).

decisions under considerable time pressure shortly after the personnel records breach was discovered. For example, those officials had to decide whether to offer identity theft services or pursue other options to mitigate identity theft risks, what services to provide, who should receive them, for how long services should be provided, and how and from whom to purchase them.

As of October 2016, the most recent version of OPM's breach-response operating manual, issued in February 2016, did not address identity theft services. OPM officials told us that they were currently in the process of drafting a policy on identity theft services, but they were waiting for OMB to issue updated guidance on the use of these services before finalizing OPM's own policy regarding these services. We have identified as a key operational practice that agencies should have procedures in place to determine what assistance, if any, should be offered to affected individuals after a data breach—including identity theft services.⁷⁴ Without a policy on when to provide identity theft services, OPM risks having to continue to make such determinations under time pressure and without guidance, hindering informed decision making on the appropriate services, if any, to offer individuals affected by a breach.

In addition, OPM officials were able to provide only very limited information and no documentation on how the agency decided to offer identity theft services after the 2015 breach of personnel records data, including any alternatives it considered. Officials told us that the OPM employees who were principally responsible for this decision were no longer employed at OPM at the time of our review. The current officials told us that they could not find any formal documentation related to the decision to offer identity theft services or the process leading up to this decision. The agency was able to identify a document comparing past public- and private-sector entities' responses to breaches that may have been considered when determining which services OPM should offer after the second data breach (of background investigation records). Agency officials told us these decisions were likely not documented because they

⁷⁴[GAO-14-34](#).

were made during a crisis, under intense pressure, and were principally the subject of oral discussions during meetings.⁷⁵

OPM does not have policies and procedures in place to provide reasonable assurance that its decision making about whether to offer identity theft services and which services to offer is documented. Our key operational practices on data-breach response note that agencies should review and evaluate their responses to data breaches, including remedial actions taken, and document lessons learned.⁷⁶ In addition, federal internal control standards state that significant events should be documented in a manner that allows the documentation to be readily available for examination.⁷⁷ Without documentation of its response to data breaches, OPM may be limited in its ability to review, evaluate, and improve its data breach response in the future, particularly when key personnel leave the agency, and it may miss opportunities to improve its decision making.

OPM Offered Duplicative Services to 3.6 Million People, and the Government Does Not Have a Process in Place to Limit Further Duplication

After the 2015 OPM data breaches, OPM offered duplicative identity theft services for approximately 3.6 million people who were affected by both breaches. Specifically, OPM awarded a contract to the Winvale Group, LLC (Winvale) in June 2015 to cover about 4.2 million people affected by its personnel records breach. In September 2015, the Naval Sea Systems Command, a component of the Department of Defense, acting on behalf of OPM, awarded a second contract to a different firm, Identity Theft Guard Solutions, LLC (doing business as ID Experts), which covered about 21.5 million people affected by the separate breach of background investigation data. OPM has estimated that about 3.6 million people were affected by both breaches and therefore were offered identity theft services under both contracts. OPM officials were not able to provide data on the number of people who signed up for both services. An official from the Naval Sea Systems Command said that recording such information is not something that an agency would typically do, or have readily

⁷⁵While OPM could not provide documentation on its decision to offer identity theft services, OPM was able to provide contract files that document, among other things, the process for procuring those services and the selection factors used in deciding to award the contract.

⁷⁶[GAO-14-34](#).

⁷⁷GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014), 48.

available, because it would require cross referencing two lists for each of the breach contracts.

The services offered by Winvale and by ID Experts are similar. Both contracts include three-bureau credit monitoring, access to an initial credit report, and identity monitoring, provided through the same subcontractor, as well as identity theft insurance and identity restoration services.⁷⁸ People affected by the breaches must enroll with the companies to receive credit and identity monitoring, but they receive the insurance and access to restoration services whether or not they enroll.⁷⁹

According to OPM, the duplicative services offered to the two groups of affected individuals overlapped by more than a year—from September 1, 2015, to December 1, 2016.⁸⁰ As discussed previously, OPM is required to provide affected individuals with coverage that is effective for at least 10 years—through at least December 18, 2025.⁸¹ According to OPM, the cost of the Winvale contract was shared between OPM and the Department of the Interior, and the cost of the ID Experts contract was paid by OPM. Both contracts were paid through OPM’s revolving fund, which contains funds collected from other federal agencies.⁸² OPM told

⁷⁸The contracts had some differences, including lengths of service (18 months versus 3 years) and coverage of dependents.

⁷⁹For both contracts, we estimated that the price was approximately \$5 per year for each person in the affected population. About 25 percent and 12 percent of those eligible enrolled in the services for the Winvale and ID Experts contracts, respectively. For both contracts, identity theft insurance and identity theft restoration services were available to the entire affected population whether or not they enrolled.

⁸⁰Coverage under the Winvale contract began on June 2, 2015. Coverage under the ID Experts contract began September 1, 2015. Coverage under the Winvale contract ended on December 1, 2016, while coverage under the ID Experts contract will likely continue through December 31, 2018.

⁸¹The Consolidated Appropriations Act, 2016, which provided for individuals affected by both breaches to receive identity theft services for the same length of time (10 years) was enacted after both of these contracts were awarded.

⁸²An intragovernmental revolving fund is an appropriation account authorized to be credited with collections from other federal agencies’ accounts that are earmarked to finance a continuing cycle of business-type operations. According to OMB, collections of intragovernmental revolving fund accounts are derived primarily from within the government. GAO, *A Glossary of Terms Used in the Federal Budget Process*, [GAO-05-734SP](#) (Washington, D.C.: September 2005). The self-sustaining nature of these accounts means that funds received in exchange for services remain available for authorized purposes without needing to be reappropriated, subject to certain conditions.

us that through November 22, 2016, about \$28.9 million was obligated under the Winvale contract, and about \$209.1 million was obligated under the ID Experts contract. OPM officials told us that the duplication ended on December 1, 2016, because the Winvale contract expired and OPM awarded a new contract to ID Experts to provide identity theft services to the approximately 600,000 people affected only by the personnel records breach. In addition, before the Winvale contract expired, OPM had modified both contracts to reduce duplication related to identity theft insurance coverage.⁸³

Other federal agencies also face the potential for such duplication. For example, in June 2015, DHS offered 18 months of free identity theft services to approximately 48,000 individuals whose information was compromised in a breach of its background investigation contractor. Because some of these individuals whose information was compromised were federal employees, they may also have been offered identity theft services by OPM.⁸⁴ Such duplication could continue to occur in the future given that OPM is required to provide identity theft services through at least December 18, 2025.

The federal government does not have a process in place to avoid offering duplicative identity theft services, although, as previously noted, OPM has addressed future duplication in its provision of identity theft services to individuals affected by the 2015 breaches. OMB's guidance on the use of identity theft services does not address whether and how agencies should consider the risk of duplication when deciding to purchase these services. While agencies report data breaches to and consult with a single federal center, the U.S. Computer Emergency Readiness Team, each breached agency makes its own decisions about offering identity theft services. OPM staff noted that addressing such duplication could involve significant practical challenges—for example,

⁸³To address duplication in insurance coverage, OPM arranged for one contractor to provide \$5 million in identity theft insurance for each of the approximately 600,000 people who were only affected by the personnel records breach and for the second contractor to provide \$5 million in insurance for each of the approximately 21.5 million people affected by the background investigation breach (including the 3.6 million who were affected by both breaches and had previously been covered by two similar insurance policies).

⁸⁴Many federal employees may also have been offered free identity theft services from nonfederal sources. For example, in March 2015, many federal employees who enrolled in the Blue Cross and Blue Shield Federal Employee Program health insurance plans were offered 2 years of free identity theft services by the insurance company Anthem after a data breach occurred at Anthem.

logistical and privacy issues may be associated with maintaining a master database of individuals who receive identity theft services across federal agencies. Further, OMB staff noted that the specific services and time frames that may be offered to individuals can vary, which presents additional challenges. However, there may still be ways to avoid duplication, such as helping coordinate the response across agencies or providing guidance intended to avoid duplication of services. Both Congress and the administration have cited the goal of reducing unnecessary duplication in the federal government.⁸⁵ The lack of a government-wide policy or process in place to coordinate the use of identity theft services across the federal government may continue to result in duplicative services that may be wasteful or unnecessary.

In the fiscal year 2017 President's budget, the administration proposed providing identity theft services to all federal employees as a standard employment benefit.⁸⁶ A staff member from OMB's Office of Performance and Personnel Management told us that this proposal would address the issue of providing duplicative identity theft services to federal employees. However, this proposal's effectiveness in addressing duplication may be limited because many data breaches at federal agencies affect people who are not federal employees, who might still be offered duplicative services if they are affected by more than one federal data breach.

Private Companies Often Offer Services after Breaches Based on Factors Other Than the Risk of Identity Theft

Private companies often offer consumers affected by a data breach complimentary identity theft services for reasons other than mitigating the risk of identity theft, such as avoiding liability, reassuring customers of their efforts to help mitigate the risk of identity theft, or complying with legal requirements. In many cases, companies offer these services voluntarily. California's Office of the Attorney General reported that in 47 percent of cases in which an entity reported a data breach in 2012 and 2013, when California law did not require offering identity theft services,

⁸⁵For example, see Executive Office of the President, *Building a 21st Century Government by Cutting Duplication, Fragmentation, and Waste* (Washington, D.C.: Feb. 28, 2012). In addition, as noted earlier, in 2010, Congress included a provision in statute for GAO to identify federal programs, agencies, offices, and initiatives with duplicative goals and activities within departments and government-wide, and report to Congress annually on the findings. Statutory Pay-As-You-Go Act of 2010, Pub. L. No. 111-139, § 21, 124 Stat. 8, 29 (2010).

⁸⁶According to OPM, as of October 2016, the agency was not aware of current or ongoing discussions to implement this proposal.

the breached entity offered free subscriptions to such services.⁸⁷

According to a 2016 report by the consulting firm Deloitte, the cost of providing free credit monitoring is one of the most commonly recognized and well understood costs that a data breach imposes on companies.⁸⁸

The services offered by private companies do not necessarily address the risks associated with a particular breach. For example, companies sometimes provide credit monitoring, which detects new-account fraud, even when only credit card information, names, and addresses have been compromised—information that does not directly increase the risk of new-account fraud. A representative of a large retailer that experienced a credit card breach involving tens of millions of consumers told us that the company decided to offer credit monitoring even though credit monitoring would not help address the consequences of the breach. This representative said that they felt they needed to provide their customers with some benefit and offered the services to give their customers peace of mind.

Some factors that may inform companies' decisions to provide identity theft services after data breaches include the following:

- **Customer satisfaction or reassurance.** Some companies told us that they offered free identity theft services to give their customers peace of mind or provide them with some benefit when notifying them that their personally identifiable information was compromised in a breach. Some reports and articles that offer advice to companies on responding to data breaches describe the offer of free identity theft services as standard practice. In addition, many states require companies to notify affected individuals about certain data

⁸⁷Kamala D. Harris, Attorney General, California Department of Justice, *California Data Breach Report* (October 2014), accessed October 31, 2016, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf.

⁸⁸Emily Mossberg, John Gelinne, and Hector Calzada, *Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts* (Deloitte, 2016), accessed October 11, 2016, <http://www2.deloitte.com/us/beneath-the-surface-of-a-cyberattack>.

breaches.⁸⁹ Companies sometimes offer identity theft services with the required notification letters.

- **Legal requirements.** Some states have requirements or recommendations related to the provision of identity theft services after a data breach. For example, Connecticut law requires entities experiencing a breach of the Social Security numbers of Connecticut residents to provide appropriate “identity theft prevention services” and, if applicable, “identity theft mitigation services,” at no cost for at least 12 months.⁹⁰ Additionally, California law provides that in breaches of Social Security or driver’s license numbers, if the person or business providing the notification was the source of the breach, an offer to provide appropriate “identity theft prevention and mitigation services,” if any, shall be provided at no cost to affected persons for at least 12 months.⁹¹ In some cases, state governments encourage entities to offer identity theft services after data breaches even when there is no legal requirement to do so. For example, a report issued by New York’s Office of the Attorney General states that while not required by law, New Yorkers affected by a data breach should be provided with mitigation services for free.⁹²
- **Liability mitigation.** Some companies may offer identity theft services to protect themselves from lawsuits. A 2014 study of data breach litigation concluded that lawsuits were less likely when the

⁸⁹Additionally, some federal laws impose information security or breach notification requirements on companies in certain industries. See, e.g., Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, Tit. XIII, § 13402, 123 Stat. 226, 260 (2009); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, Tit. V, 113 Stat. 1338, 1436 (1999); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (1996). The Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation have also issued interagency guidance for financial institutions subject to the Gramm-Leach-Bliley Act on response programs when data breaches occur. See 12 C.F.R. pt. 30, App. B; 12 C.F.R. pt. 170, App. B; 12 C.F.R. pt. 208, App. D-2; 12 C.F.R. pt. 225, App. F; 12 C.F.R. pt. 364, App. B.

⁹⁰Conn. Gen. Stat. §§ 36a-701b, 38a-999b. The requirement to offer such services applies when the resident’s Social Security number was breached or is reasonably believed to have been breached.

⁹¹Cal. Civ. Code § 1798.82(d)(2)(G).

⁹²New York State Office of the Attorney General, *Information Exposed: Historical Examination of Data Breaches in New York State* (July 15, 2014), accessed July 15, 2016, http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf.

breached company offered credit monitoring or identity theft insurance.⁹³

When selecting a vendor to provide identity theft services, companies consider a variety of factors, but generally do not directly assess the effectiveness of each provider's services, according to breached companies and experts with whom we spoke. Key selection factors that they cited included price, reputation, capacity to respond quickly to large-scale breaches, and ability to provide comprehensive post-breach services, such as complying with statutory notification requirements.

Conclusions

The identity theft services that are currently available have some benefits, but a number of limitations, and alternatives are available at little or no cost. We found issues with the federal approach to offering identity theft services in several areas. The requirement for OPM to provide individuals affected by the breaches it announced in 2015 with \$5 million in identity theft insurance may impose future potential costs and have other consequences—without providing a meaningful corresponding benefit. The \$1 million in coverage previously provided was almost certainly adequate based on available claim information, which indicates that claims against identity theft insurance are few in number, and claims paid appear to rarely exceed a few thousand dollars. Although the goal for mandating \$5 million in identity theft insurance was to provide additional protection to employees, mandates such as this may not be aligned with stated goals of generally reducing unnecessary spending. In the event that future requirements are imposed on agencies to provide identity theft insurance, allowing the agency to determine the level of coverage would likely result in a lower and more appropriate coverage amount. This would be more cost-effective, avoid creating a misimpression among consumers that the scope of coverage is broader than it is, and help prevent an unwarranted escalation of the amount of coverage in the marketplace for identity theft services.

Further, under FISMA, OMB is required to oversee agency information security policies and to ensure that data breach notification policies and guidelines are updated periodically. OMB's January 2017 guidance memorandum provides a brief discussion of some of the potential benefits and limitations of identity theft services. However, this guidance does not

⁹³Sasha Romanosky, David Hoffman, and Alessandro Acquisti, "Empirical Analysis of Data Breach Litigation," *Journal of Empirical Legal Studies*, vol. 11, no. 1 (2014).

address the effectiveness of these services relative to lower-cost alternatives or countermeasures, such as credit freezes or an agency conducting its own monitoring of databases related to compromised data. As a result, the guidance may not ensure that agencies offer these services only when they are certain to be a useful and cost-effective response to a data breach—contrary to OMB’s risk management and internal control guidance that federal leaders identify goals and risks, and appropriately respond to improve effectiveness and efficiency.

In addition, OPM’s offer of duplicate services to approximately 3.6 million people demonstrates the need to address potential duplication of identity theft services. Currently, agencies’ decisions to offer these services are made without consideration of whether affected individuals already receive such coverage. We acknowledge that logistical and privacy issues present challenges in addressing this duplication. Nevertheless, because federal agencies may continue to provide duplicative coverage to some individuals, an exploration by OMB of viable options to mitigate the risk of duplicative coverage is warranted—and would be consistent with OMB’s stated goal of cutting duplication across the federal government to improve efficiency and save taxpayer dollars.

Finally, OPM was hindered in its ability to address its 2015 data breaches because it does not have a policy on when and whether to offer identity theft services, requiring decision making under time pressure without pre-established guidance. Further, OPM’s failure to adequately document how it made these decisions is inconsistent with federal internal control standards, which call for documentation of significant events to enable later review, and with our key practices for data-breach response, which include reviewing past breach responses to improve policies and benefit from lessons learned. Having a policy in place to guide decisions about when and whether to provide identity theft services or other forms of assistance to people affected by a breach, and documenting decisions made about such assistance, could improve OPM’s approach to providing assistance after future data breaches.

Matter for Congressional Consideration

In the event that Congress again requires an agency to provide affected individuals with identity theft insurance in response to a breach of sensitive personal data, Congress should consider permitting the agency to determine the appropriate level of that insurance.

Recommendations for Executive Action

We recommend that the Director of the Office of Management and Budget take the following two actions:

- to the extent feasible, conduct an analysis of the effectiveness of the various identity theft services relative to alternatives, and revise OMB's guidance to federal agencies in light of this analysis; and
- explore options to address the risk of duplication in federal agencies' provision of identity theft services in response to data breaches, and take action if viable options are identified.

We recommend that the Director of the Office of Personnel Management take the following two actions:

- incorporate criteria and procedures for determining whether to offer identity theft services into the agency's data-breach-response policy; and
- implement procedures that provide reasonable assurance that significant decisions on the use of identity theft services are appropriately documented.

Agency Comments and Our Evaluation

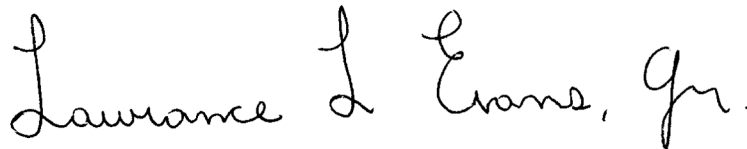
We provided a draft of this report to CFPB, Department of Defense, Department of Justice, FTC, GSA, OMB, OPM, the Postal Service, and VA for review and comment. In written comments, which are reprinted in appendix III, OPM said that it concurred with our two recommendations to the agency. OPM said it will be updating its data breach response plan, in accordance with OMB's recent guidance, by July 2017. OPM expects this plan to address our recommendations to incorporate criteria and procedures for determining whether to offer identity theft services and to implement procedures to document the agency's decision making in that regard.

In comments provided orally, staff from OMB's Office of Information and Regulatory Affairs said that our draft recommendation to OMB on

expanding OMB's guidance to federal agencies would benefit from greater specificity, and we revised this recommendation to provide greater clarity. With regard to our recommendation on addressing duplication, staff highlighted the challenges of doing so, and in response we modified the recommendation and added additional material acknowledging these challenges. In addition, staff from CFPB and FTC provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to CFPB, Department of Defense, Department of Justice, FTC, GSA, OMB, OPM, the Postal Service, VA, the appropriate congressional committees and members, and others. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact me at (202) 512-8678 or evansl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

A handwritten signature in black ink that reads "Lawrence L. Evans, Jr." The signature is written in a cursive, flowing style.

Lawrence L. Evans, Jr.
Director, Financial Markets and Community Investment

List of Requesters

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Digital Commerce and Consumer Protection
Committee on Energy and Commerce
House of Representatives

The Honorable Tim Murphy
Chairman
The Honorable Diana DeGette
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Michael Burgess, M.D.
House of Representatives

The Honorable Fred Upton
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The objectives of this report were to examine (1) the marketplace for identity theft services; (2) the potential benefits and limitations of identity theft services available to consumers; (3) marketing, billing, and security issues associated with these services; and (4) factors that affect government and private-sector decision making about offering identity theft services. For the purposes of our review, we use the term “identity theft services” to refer to commercial products that generally provide tools that are intended to help consumers detect identity theft and restore their identity if it has been compromised. There is no standard term to describe these services, which sometimes are also referred to as “identity theft protection services,” “identity protection services,” “identity monitoring services,” and “credit monitoring services,” among other variations.

To examine the marketplace for identity theft services, we used Internet search techniques and keyword search terms to identify sources and types of available information about the identity theft services industry, including the number and nature of companies providing these services, industry revenues, product offerings, and how the services are sold to and priced for consumers. In doing so, we identified and reviewed studies on identity theft services conducted by consumer advocacy groups, private research firms, and nonprofit organizations, including the Consumer Federation of America, Javelin Strategy & Research, Ponemon Institute, and RAND Corporation.¹ In addition, we searched online research databases, including Nexis and ProQuest, using as search terms the names of large identity theft service providers and products, which provided news articles, annual public filings, and other information. We analyzed U.S. Census Bureau data to obtain information on business classification codes (including Standard Industrial Classification and North American Industry Classification System codes) assigned to identity theft service providers to classify their main industry and line of business. On the basis of our analyses, we determined that the Census data do not provide a reliable count or other statistical information on the identity theft services industry, and that publicly available information about the industry as a whole is limited.

In addition, we collected and analyzed product information from the websites of 26 identity theft services, which represented nearly all such

¹Consumer Federation of America is a consumer research, advocacy, education and service organization. Javelin Strategy & Research and Ponemon Institute are private research groups. The RAND Corporation is a nonprofit, nonpartisan research organization.

companies providing these services that we identified through our review of studies described previously, and included providers who have been awarded federal contracts and been party to federal enforcement actions.² In some instances, we spoke with the providers to gather additional information or clarify certain aspects of the products. We generally did not independently verify this information, but we did use it for context and to provide a broader picture of available products and key features. To collect pricing information on identity theft services' direct-to-consumer services, we used information from our review of 26 identity theft services' websites, and reviewed a subset of five large providers' websites for more detailed pricing information. To identify prices for post-breach identity theft services marketed to the federal government, we reviewed the General Services Administration's (GSA) identity theft services blanket purchase agreements, and we corresponded with two of the three participating contractors.

To examine the potential benefits and limitations of identity theft services, we reviewed and summarized available reports, documents, congressional testimonies, position papers, and education materials from consumer protection agencies, consumer advocacy groups, private research firms, providers, and others. We also used information collected in our review of 26 identity theft services' websites. We collected and reviewed the terms, conditions, and exclusions of at least one identity theft insurance policy from each of five providers, selected because they were among the largest market participants, and interviewed representatives of an insurance company that is a market leader in identity theft insurance. In addition, we reviewed reports that seek to rate and evaluate identity theft services that were issued by consumer groups, private research firms, and industry analysts.

To examine marketing, billing, and security issues associated with identity theft services, we reviewed consent orders, press releases, and settlement agreements related to federal enforcement actions associated with identity theft services. We also reviewed the comment letters submitted in response to the Bureau of Consumer Financial Protection's (CFPB) March 2015 request for public comment related to credit card

²We included only companies that operate identity theft services, but not other companies (such as financial institutions) that offer their customers these services by partnering or contracting with an identity theft service provider.

add-on products such as identity theft services.³ In addition, we reviewed companies' annual report public filings with the Securities and Exchange Commission (Form 10-K) from five large publically traded identity theft service providers to identify issues related to safeguarding data.⁴

Furthermore, we reviewed three studies conducted by the Consumer Federation of America that examined the websites and other aspects of selected identity theft services. We also conducted our own review of the websites of 10 identity theft service providers, which were selected to represent a mix of services and included some of the largest, as well as some of the smaller industry participants.

In addition, we collected information on the number of consumer complaints by requesting from the Federal Trade Commission (FTC) a search of its Consumer Sentinel Network database, which includes complaints submitted to FTC, CFPB, the Better Business Bureaus, and other sources. The search we reported on covered calendar year 2015 and used the word strings "credit monitoring," "identity protection," "identity theft protection," "ID protection," and "ID theft protection." (The search resulted in approximately 3,000 complaints, but we estimated that 2,500 were related directly to identity theft services after identifying about 500 that were related to fraud alerts.) To better understand the nature of the complaints, we reviewed the narrative associated with complaints, as available, and CFPB's subcategories for complaints related to identity theft services in CFPB's consumer complaint database from December 2011 to June 2016. In addition, we received complaint data from the Council for Better Business Bureaus from April 2013 to April 2016 for complaints identified under its "identity theft protection and prevention services" business category, including the complaint category that was assigned to each complaint (e.g., billing, service, advertising issues). We assessed the reliability of the complaint data by interviewing agency officials; reviewing relevant documentation; analyzing complaint narratives; and comparing data from the three different sources. We found the data to be reliable for purposes of this report. However, in general, consumer complaint data have limitations as an indicator of the extent of problems. For example, not all consumers who experience

³See Request for Information Regarding Credit Card Market, Notice and Request for Information, 80 Fed. Reg. 14,365 (Mar. 19, 2015).

⁴Federal securities laws require public companies to disclose information on an ongoing basis. These disclosures include the annual report on Form 10-K, which provides a comprehensive overview of the company's business and financial condition and includes audited financial statements.

problems may file a complaint, and not all complaints are necessarily legitimate or categorized appropriately. In addition, a consumer could submit a complaint more than once, or to more than one entity, potentially resulting in duplicate complaints.

To assess factors that affect government and private-sector decision making about offering identity theft services, we reviewed documentation from, and interviewed representatives of, three federal agencies—the Office of Personnel Management (OPM), Department of Veterans Affairs, and the U.S. Postal Service—and interviewed representatives from three private companies that had experienced data breaches and offered identity theft services to affected individuals. The factors considered in selecting these six entities included the number of records breached, sensitivity of the data breached (e.g., Social Security numbers, health information, credit card numbers), when the breach took place, and whether identity theft services were procured as a result of the breach. We also spoke with GSA and Naval Sea Systems Command because they had administered identity theft services contracts for federal agencies. We reviewed relevant laws and regulations, federal guidance, federal data breach policies, and contract documentation, including contracts, solicitations, and performance reports. Most of the private entities we initially contacted were not willing to speak with us due to ongoing litigation. Therefore, we asked identity theft service providers to help us identify alternate private entities that had purchased identity theft services in response to a data breach. The three private companies that had experienced a breach with whom we spoke were a large retailer, a financial institution, and a health care provider.

To address all objectives, we interviewed representatives of CFPB, FTC, the Department of Justice, GSA, Naval Sea Systems Command, the Office of Management and Budget, and OPM. We also interviewed representatives of the Council for Better Business Bureaus, Consumer Federation of America, Medical Identity Fraud Alliance, National Consumer Law Center, Consumer Data Industry Association, and the National Association of Insurance Commissioners, as well as experts in security or identity theft services. These entities and individuals were selected because of their involvement and expertise in the area of identity theft services. In addition, we interviewed representatives of eight companies that provide identity theft services—AllClear ID, CSID, Equifax, Experian, ID Experts, IDShield, LifeLock, and Winvale—which were selected because they represented most of the largest market participants, included the contractors used to provide identity theft services for the 2015 OPM data breaches, and offered a mix of products.

We conducted this performance audit from September 2015 to March 2017, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Selected Federal Laws Potentially Applicable to Identity Theft Services

Certain federal laws and regulations that govern the sharing and protection of personal information, and that prohibit unfair or deceptive acts or practices, may be applicable to identity theft services and the companies that offer them, depending on the circumstances. These include the following:

- *The Gramm-Leach-Bliley Act (GLBA)* contains provisions that restrict, with some exceptions, the disclosure of nonpublic information by entities that fall under GLBA's definition of a financial institution or that receive nonpublic personal information from a financial institution.¹ GLBA generally requires financial institutions to provide notice and an opportunity for consumers to opt out before sharing their nonpublic information with nonaffiliated third parties, other than for certain purposes such as processing a financial service authorized by the consumer. Regulations implementing GLBA also require financial institutions to develop, implement, and maintain a comprehensive information security program; monitor, test, and adjust the program as needed; and designate a person in charge of the security program.² Federal Trade Commission (FTC) officials told us that many companies that provide identity theft services do not fall under the GLBA safeguarding rules because they are not financial institutions as defined by GLBA. However, financial institutions that offer identity theft services as an add-on product in conjunction with credit cards would be subject to GLBA requirements.
- *The Fair Credit Reporting Act (FCRA)* protects the security and confidentiality of personal information collected or used for eligibility determinations for such purposes as credit, insurance, or employment.³ FCRA limits the use and distribution of personal data collected for consumer reports, allows individuals to access and dispute the accuracy of personal data held on them, and imposes safeguarding requirements for such data. FCRA imposes certain

¹Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of titles 12 and 15 of the U.S. Code).

²See, e.g., 16 C.F.R. pt. 314 (FTC's Standards for Safeguarding Customer Information). Other agencies, including Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, and Securities and Exchange Commission, have also established safeguards standards under GLBA for the financial institutions under their respective jurisdictions.

³Pub. L. No. 91-508, Tit. VI, 84 Stat. 1114, 1128 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x).

duties on those entities meeting the definition of consumer reporting agencies under the act, which includes the three nationwide consumer reporting agencies (commonly called credit bureaus) and other businesses that collect or disclose information for consumer reports for use by others.⁴ These duties would not be imposed on companies that provide identity theft services if they do not meet the statutory definition of consumer reporting agencies. FCRA also imposes certain duties on users of consumer report information.

- *The Credit Repair Organizations Act* prohibits untrue or misleading representations and requires certain affirmative disclosures in the offering or sale of credit repair services.⁵ Some courts have held that entities offering credit monitoring services in some circumstances fit within the act's definition of credit repair organizations and are therefore subject to the act's requirements.⁶
- Section 5 of the *Federal Trade Commission Act* (FTC Act) authorizes FTC to take action against unfair or deceptive acts or practices in or

⁴The Fair Credit Reporting Act defines a consumer reporting agency as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f). The act defines a consumer report as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 604 [of the act], subject to certain exclusions. 15 U.S.C. § 1681a(d).

⁵Pub. L. No. 104-208, § 2451, 110 Stat. 3009-456 (1996) (codified at 15 U.S.C. §§ 1679-1679j).

⁶See, e.g., *Helms v. ConsumerInfo.com, Inc.*, 436 F. Supp. 2d 1220, 1232-34 (N.D. Ala. 2005) (holding that an organization providing credit monitoring services for money and representing that its services will improve a customer's rating was a credit repair organization subject to the Credit Repair Organizations Act). See also *Stout v. FreeScore, L.L.C.*, 743 F.3d 680, 687 (9th Cir. 2014); *In re National Credit Mgmt. Group, L.L.C.*, 21 F. Supp. 2d 424, 458 (D. N.J. 1998). Under the Credit Repair Organizations Act, a credit repair organization is any person who sells, provides, or performs, or represents that it can or will sell, provide, or perform, any service, in return for payment, for the express or implied purpose of improving any consumer's credit record, credit history, or credit rating; or providing advice or assistance to any consumer with regard to any such activity or service, subject to exceptions. 15 U.S.C. § 1679a(3).

affecting commerce.⁷ The Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and the National Credit Union Administration also have the authority to enforce the FTC Act for institutions under their respective jurisdictions.⁸ The FTC Act does not contain specific requirements for identity theft services or any other products, but FTC has interpreted the act to apply to companies' violations of their written policies, including policies on how they use or share personal information.

- The *Consumer Financial Protection Act* of 2010 prohibits unfair, deceptive, or abusive acts or practices by those entities, or their service providers, that offer or provide consumer financial products or services.⁹ It also authorizes the Bureau of Consumer Financial Protection (CFPB) to take enforcement actions to prevent those who offer or provide consumer financial products or services from engaging in unfair, deceptive, or abusive acts or practices in connection with transactions with consumers involving consumer financial products or services or the offering of consumer financial products or services.¹⁰

⁷38 Stat. 717, § 5 (1914) (codified as amended at 15 U.S.C. § 45). The FTC Act further provides that an act or practice is "unfair" if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). The act does not provide a standard of what constitutes a "deceptive" act or practice, but FTC has issued guidance stating that it will find deception where there is "a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." See FTC Policy Statement on Deception, October 14, 1983.

⁸The Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation can enforce the FTC Act under the Federal Deposit Insurance Act, 12 U.S.C. § 1818, and the National Credit Union Administration can enforce the FTC Act under the Federal Credit Union Act, 12 U.S.C. § 1786.

⁹Pub. L. No. 111-203, §§ 1031, 1036, 124 Stat. 1376, 2005, 2010 (2010) (codified at 12 U.S.C. §§ 5531, 5536).

¹⁰In accordance with a memorandum of understanding, CFPB and FTC endeavor to coordinate law enforcement activities under the Consumer Financial Protection Act and the FTC Act respectively, including conducting joint investigations where appropriate, to minimize duplication of efforts and burden on investigation subjects. These actions may include claims brought by FTC against nonbanks subject to its jurisdiction. As to the laws CFPB enforces, staff told us the determination of whether CFPB has authority over identity theft service providers that are not covered banks would be determined on a case-by-case basis and would largely depend on the services they provide and their line of business.

Appendix III: Comments from the Office of Personnel Management



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

FEB 22 2017

Lawrence L. Evans, Jr., Director
Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Evans:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, *Identity Theft Services: Services Offer Some Benefits but are Limited in Preventing Fraud*, GAO-17-254.

The Office of Personnel Management (OPM) takes seriously its responsibility to effectively respond to any breach of the personally identifiable information we hold. Pursuant to the Office of Management and Budget's (OMB) recently issued Memorandum 17-12 (OMB M-17-12), this includes carefully evaluating the risk of harm to individuals who may be affected by a breach and determining how best to mitigate that harm. To that end, OPM is committed to ensuring that we have consistent criteria by which to evaluate every breach and an appropriate process in place to document our decisions.

Responses to your recommendations are provided below.

Recommendation 1: GAO recommends that the Director of OPM incorporate criteria and procedures for determining whether to offer identity theft services into the agency's data-breach-response policy.

Management Response:

We concur. OPM will update its breach response plan in accordance with OMB M-17-12. That memorandum requires that OPM assess the risk of harm to individuals affected or potentially affected by a breach and to determine how best to mitigate that harm, including what services to offer affected individuals. The framework set out in the memorandum for conducting those assessments will be incorporated into the OPM breach response plan, which is due to be completed and submitted to OMB by July 2017.

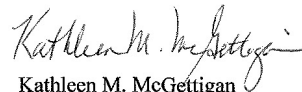
Recommendation 2: GAO recommends that the Director of OPM implement procedures that provide reasonable assurance that significant decisions on the use of identity theft services are appropriately documented.

Management Response:

We concur. As noted above, OPM will update its breach response plan in accordance with OMB M-17-12. In developing that plan, OPM will incorporate the memorandum's guidance concerning tracking and documenting the agency's response to a breach, including documenting decisions to provide identity theft services to affected individuals. The OPM breach response plan is due to be completed and provided to OMB by July 2017.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Kellie Cosgrove Riley, Chief Privacy Officer, at 202-606-2308 or kellie.riley@opm.gov.

Sincerely,



Kathleen M. McGettigan
Acting Director

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Lawrance L. Evans, Jr., (202) 512-8678 or evansl@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jason Bromberg (Assistant Director), Theodore Alexander, Shamiah Kerney, and Verginie Tarpinian made key contributions to this report. Also contributing to this report were JoAnna Berry, Marc Molino, Patricia Moye, Stephen Robblee, Jennifer Schwartz, Andrew Stavisky, and Tatiana Winger.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [LinkedIn](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov and read [The Watchblog](#).

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.